EMAIL AND TEXT SPOOFING AND SCAMS

More and more congregations, and ministries are being targeted by scammers and phishing attacks. These emails or text messages often pretend they are a pastor or bishop and ask for private conversation, or the need to for a favor, or to purchase gift cards.

These attacks are a phishing or spoofing scam. This means that the email account or phone number has probably NOT been hacked. Attackers are using an alternate email address or phone number and contacts found using A.I. software.

This kind of attack is often called CEO Phishing or Business Email Compromise. In 2019, the FBI reported that this is a $26 billion scam.

HOW IT WORKS

The attackers decide on a target (a congregation, ministry or synod) and does a search for names and email addresses of leadership.

The attackers create email addresses with a convincing name or domain to look similar to that of the leadership.

They then use software to find email addresses or phone numbers associated with their target.

They send emails or texts to the found addresses posing as a pastor or bishop to solicit money or information.

HOW TO AVOID OR STOP SCAMS

1. **Check the email address or phone number that sent the message.** Modern email programs often only display the name as a default and not the email address. The attackers use this to their advantage and create addresses with the real name but use a bogus email address. Often using gmail or yahoo accounts. Text scammers will use area codes that are in the area you are in, claiming it is a new phone number.

2. **Look for red flags in the tone and grammar of the email or text.** Attackers will want to create a sense of urgency, to prey on your desire to help. They will often claim the bishop or pastor needs something and is in a meeting. Or needs to urgently have a private conversation. These emails will often contain misspellings, strange punctuation, or grammar that is just "off" a bit. Read messages with requests carefully.

3. **Ask someone.** Have someone else read the message for you to see if they notice anything weird. Call or email the church or synod office to check what the email address or phone number of person actually is.

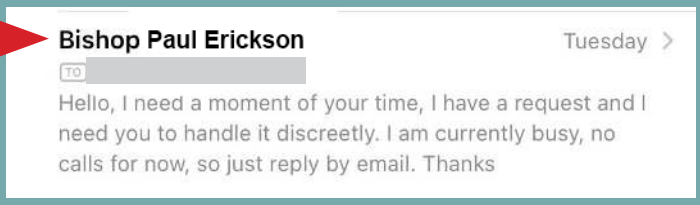
4. Do not purchase gift cards or give out information. These scams often ask for the purchase of gift cards or want you to provide further information (for more scams). Never share information or make purchases from a text or email request without verifying information.

5. Report it. Report it to the person or leadership, the chances good that if you received a scam email or text, someone else did too. Also report it to the FCC. If you are the victim of a scam, report it to local law enforcement.

SOME EXAMPLES

These are scam emails and texts

This is how one of these fake emails looks in a mail app on a phone, notice that the email address isn't displayed



This is a scam text. Notice the sense of urgency. This text came from an unknown number.

RESOURCES

- From the FBI: Business Email Compromise
- From the FBI: Gift Card Scams
- From the ELCA: Tips for Computer and Internet Security
- From the ELCA: Information Security Webinar
- Security Awareness: Article about messaging attacks
- Blog post with more examples of phishing attacks

REPORT SCAMS

- Report spoofed or fake gmail addresses to Google
- File a complaint to the FCC
- If you are a victim of one of these scams contact local law enforcement and file a claim with the FBI Internet Crime Complaint Center

With thanks to Bishop Amy Current and the Southeastern Iowa Synod for permission to use and edit for the Greater Milwaukee Synod.