Texas District Privacy Policy

Purpose

This policy explains the types of information which the Texas District of The Lutheran Church—Missouri Synod (Texas District, LCMS) may collect about you, how we might use that information, who we might share it with, and the choices you have regarding the updating of your information.

Personal Identifiable Information

When you provide us with your personal information, we will respond to your inquiry or request. We may also contact you via Constant Contact to provide newsletters, reports or statements, which contain information regarding activities and programs that might interest you. This is to serve you best and be good stewards of district resources. When you receive such email information, you have an opportunity to update how often you receive information or decline any further information.

Credit Card Transactions

The Texas District, LCMS is able to accept a number of credit cards for the purposes of making a charitable contribution in support of our various ministries or to register for Texas District, LCMS supported events. Users are allowed the opportunity to store their credit card information for ease with future transactions within ACS (contributions) or Eventbrite (supported events). Texas District, LCMS employees do not have access to stored credit card information.

The Texas District, LCMS will not share any of your personal information with any outside party, except where required by law. We will not rent, sell, lend or provide mailing lists, telephone numbers, mailing addresses or email addresses to others outside the organization.

PROTECTING AGAINST ONLINE SCAMS
Texas District Security Document

Keeping you safe

Have you received an unexpected or unusual email, text, or other message from the Texas District? This communication is meant to help you discern legitimate messages from scams, as well as to inform you of District policies meant to minimize the possibilities of fraud.

There are two main types of malicious messages: Malicious payload and Social Engineering

Malicious payload

The goal of these emails (and text messages) is to run malicious software on your computer so that the criminal can take actions on your system. They typically contain malicious links or attachments that will attempt to get you to click or open.

Social Engineering

The goal of these messages is to trick you into sending the thieves money, or sharing private details such as bank account numbers, credit card numbers, social security numbers, etc.

Spear phishing is a common variety - these are highly targeted emails (or text messages, or even phone calls) purporting to be from someone trusted - your boss, your pastor, your friend, tech support (e.g., Microsoft, Apple, Norton Anti-virus), financial services (Amazon billing, Bank of America fraud, Social Security Administration, your utility company), the police or FBI.

The email or text message will often be from a free account. e.g., instead of an @txlcms.org address, the address might be something like President687[at]gmail.com. That said, many email systems will hide the sender's address, so you might only see something like "President Newman" or

"Amazon Fraud Services". Sometimes they will hack a legitimate account and send from there. Regardless of the source of the impersonation, the best step you can take to verify an email or text message is to close the message and respond Out of Band or OOB.

How to Protect Yourself?

Out Of Band or OOB confirmations will almost always succeed in defeating these types of attacks. This means responding by some other method than the original message. If you get an email, call the sender, but from your own phone book, not with any phone number provided in the original email. If the original message is a phone call, hang up and login to check your account from your own bookmark, or call back from a number you look up yourself. (e.g., look up the service number for your bank from the back of your credit card, and call that 800 number.) That takes control away from the scammers and gives it back to you.

Take Your Time and Don't Give into Urgency

If you get an email, text, or phone call scam, a common theme you will see is urgency. The scammers want to scare you into acting without pausing to think things through for many reasons. You might get a message saying someone is stranded, or their phone is broken so call at this alternative number instead of a real number. They might even attempt to run these scams when they know your boss, or some authority figure is unavailable. If they can see on social media that someone is on a flight, on vacation, or otherwise unavailable, that is a prime time to strike. This is not a time for us to follow instructions sent by email blindly, but instead to check with others.

The Texas District has policies to prevent fraud & practice good stewardship, they include:

1. The Texas District will *never* direct someone to purchase gift cards or digital currency such as bitcoin.

2. The Texas District will *never* initiate any other type of financial transaction by email.

3. Communication from District staff will always come from a txlcms.org email address. If you receive a District email communication from a free address such as gmail.com or hotmail.com, it is not a legitimate message.

3. Email addresses can be complicated and impersonated. If you receive a suspicious email from any Texas District staff person, you can forward it to verify@txlcms.org for anonymous, confidential verification.

4. Texas District staff will never send you a message asking you not to call to verify a message. We encourage just the opposite. If you receive a message asking you not to call to verify a message, the message is phishing. Please forward it to verify@txlcms.org to report it.

5. To prevent the sending of messages from a hacked txlcms.org account, all District accounts are protected with both long passwords and 2 Factor Authentication (2FA). We encourage everyone to similarly protect their email and other important computer accounts.

We Encourage you to do the Same

Online safety requires more than just technical measures and must include training and sound processes. The Texas District strongly encourages your congregation to publish a document like this, and to send it to members and publish a copy on your website, as part of your security policy and training. We all become safer by following prudent practices that inform and protect each other.