

Avoid Scam Messages

The church office has been made aware of scam messages being sent to church members using Pastor Cindy's and Pastor Lauren's names. Several people have also received messages from congregation members.

If you have received any messages that you think may be scams, please report them as such! Do not respond to the message. If you're not sure if the message is legitimate, please reach out to the church office directly and we will help you. Or, you can read the information below and follow the steps.

If you have further questions, please read this document carefully and let Kate in the church office know if you have any questions or concerns. She's happy to help in any way.

- 507-645-7532
- church@firstucc.org

Scams vs Phishing vs Spam Messages

So what's really the difference between the two anyway?

The easiest way to put this is all phishing is a type of scam, but not all scam is phishing. Basically, scams are a broad category of tricky and deceptive tactics used against people. Phishing is a branch in that category.

Scams can be used in a wider range and are not always used online. They are typically used for monetary gain. Scams include:

- Pretending to be someone else
- Offering unrealistic opportunities
- Creating a sense of urgency
- Requesting unusual payment methods

Phishing messages are types of cybercrimes and are usually conducted online. They are sent in order to gain personal information such as addresses, passwords, bank information, SSN numbers, and more. They are often sent from people impersonating legitimate organizations or people you may know. Phishing also includes fake websites.

Spam messages are repeated unsolicited messages from unwanted senders. They can be sent via email, mail, text, or phone call. They can be frustrating. They are mainly interested in selling products or services, or may be trying to get sensitive information.

Avoid/Do Not

The church staff will never send anyone a personal message from anything other than church emails ending in “*firstucc.org*.” If you do receive a strange message claiming to be from any church staff member(s), do not:

- Open emails claiming to be from pastors that don’t end in “*firstucc.org*”
- Respond to the message
- Agree to buy anything
- Click on any links or attachments in the message
- Share any personal information or passwords

Warning Signs

Emails from church staff will always be professional, polite, and respectful. We will never send personal or individual messages asking for money or favors. If you’re not sure if it’s a legitimate message, here are some warning signs to look out for:

- Urgency or pressure to act right away
- Incorrect grammar, punctuation, and/or spelling
- No salutation, sign-off, or signature confirming the message’s source or sender
- Specific instructions stating how to pay or communicate
- Inappropriate/unprofessional requests or questions
- Suspicious links

Protect Yourself and Your Family

While it’s almost impossible to not receive such emails, there are several ways to protect yourself from getting scammed:

- Call the church office if you receive a message claiming to be from a pastor or church staff member. We’ll be able to tell you if it’s legitimate or not.
- Report a phishing/scam email as soon as possible to your email host
 - Google, Yahoo, Outlook, etc.
- Secure your personal information
- Keep your software updated and use strong passwords
- Trust your gut. If it feels strange or doesn’t sound legitimate (like the person you’re emailing with), there’s a good chance it’s a scam.
 - Example: Pastor Cindy will always use proper grammar, spelling, and punctuation. She is also unlikely to use “God Bless” in her email signature. If there is improper grammar, spelling or punctuation, or “God Bless,” it may not be Pastor Cindy who sent the email.

So what can the church do?

- We can keep you updated on scams and phishing emails and make sure you have the information necessary to keep yourself and your family safe.

- Kate in the church office can give detailed information about how to report phishing attempts.
 - She can also personally walk those who may need assistance through the steps of reporting.

Because our church has a large online presence, it is possible for hackers to gain access to information we'd prefer they don't have. Keep yourself and others safe by using the best practices laid out above.

The church cannot report on scam or phishing emails sent to congregants. Congregates who receive such emails must personally report them to their email domain (Gmail, Yahoo, Outlook, etc) or to the Federal Trade Commission (FTC).

First United Church of Christ in Northfield does not hold responsibility for those who get scammed due to these messages, nor are we able to report these messages unless we receive them directly.

Helpful Links:

Federal Trade Commission:

<https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/phishing>

Reporting Phishing on Gmail:

<https://support.google.com/mail/answer/8253?hl=en>

Phishing Attacks (Imperva)

<https://www.imperva.com/learn/application-security/phishing-attack-scam/>