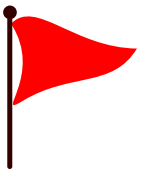
LEARN CONNECT SERVE
FLOURISH
MISSION PRESBYTERY

SCAMMER RED FLAGS

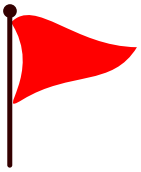
how to avoid phishing and spoofing scams

A phishing or spoofing scam pretends to be a person, church, or organization that you trust to trick you into giving away money or sensitive personal information. They often target church leaders and members, but these red flags can help you spot them.



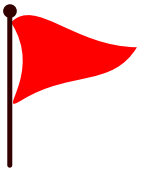
Asks for gift cards, cryptocurrency or wire transfer

A church leader will never ask you for money in any of these forms, and will not contact you individually asking for money "as a favor".



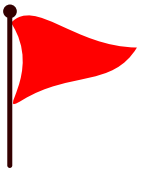
Makes everything sound very urgent and secretive

A scammer tries to get you to act fast and without talking to anyone to prevent you from thinking clearly.



Suspicious email or phone number

It may seem like the request is coming from a trusted person, but if you look closely, the address may be strange. Scammers are getting better at recreating emails and phone numbers though, so don't fully rely on this.



Uses unusual language or grammatical errors

The communication may be worded in an usual way, have a lot of spelling or grammatical errors, or just feel different than the person usually communicates. If something feels off, stop and verify.

If you think you might have received a scam, DO NOT click on any links, open any attachments, or give any information. If you're not sure, contact the person or organization directly to verify. Show it to someone. Ask for help!