

The 7 Church Scam Warning Signs Every Staff Member Should Know

You do not have to be a technology expert. Slow down, notice the warning signs, and verify before you act.

1

An unexpected request from a pastor or church leader

A text or email may use a real leader's name and sound familiar. If the request is unusual - especially if money or private information is involved - do not assume the message is genuine.

2

Pressure to act right now - or keep it secret

Scammers often create urgency, fear, sympathy, or secrecy: an emergency, a hospital situation, a mission need, a surprise, or a deadline. Pressure is a reason to slow down.

3

A request for gift cards, wire transfers, or unusual payment methods

Gift-card requests are a classic impersonation scam. Be especially suspicious when someone asks you to buy cards and send the numbers or PINs.

4

A vendor suddenly changes where the church should send money

A familiar-looking invoice can contain new bank, routing, mailing, or payment instructions. Never change payment details based only on an email. Confirm with the vendor another way.

5

The address, link, or phone number is a little different

The display name may look right while the real email address is wrong. A link may imitate a trusted website. Caller ID can also be spoofed. Look past the name on the screen.

6

The voice or message sounds exactly like someone you know

AI can make impersonation more convincing. Do not try to become an AI detective. If a request involves money, access, passwords, or sensitive information, verify it through a trusted contact method.

7

An authority figure demands immediate payment or information

Messages pretending to be the IRS, a bank, law enforcement, a charity, or another trusted organization may threaten consequences or demand quick action. Unexpected pressure is a warning sign.

STOP. CHECK. CONFIRM.

STOP

Do not click, pay, reply, or share information.

CHECK

Look for pressure, unusual requests, changed payment details, addresses, links, or numbers.

CONFIRM

Contact the person or organization another way using information you already trust.

One simple church policy: Never approve an unexpected payment request, gift-card purchase, or change in payment instructions from a text or email alone. Verify it using a second, trusted method.

Sources: Federal Trade Commission guidance on worshipper gift-card scams and AI voice-cloning risks; FBI guidance on Business Email Compromise; IRS 2026 Dirty Dozen scam guidance. Educational resource - not legal, tax, or cybersecurity advice.

[ScamSmartChurch.com](https://scamsmartchurch.com) | [Scam Demonstration Lab](#) | [Stop. Check. Confirm.](#)