



Dear State College Alliance Church

We have been made aware of several recent emails seemingly sent on behalf of the pastors or church members requesting money, gift cards, or personal information. These emails are scams, and are becoming increasingly sophisticated and frequent. Below is some guidance on how to recognize and deal with emails like this so your finances and personal info remains safe.

How do I recognize a scam email? We have seen two types of scam emails increase of recently:

- **Personal requests from a "Pastor"** These usually look like personal emails and may include accurate details like the name of a pastor, the address of the church, or other references to public information about our congregation. They usually start with just a "Please let me know if you can help with something", then if you respond they will ask for money or gift cards, still pretending to be a pastor.
- **"Exclusive Invitations"** These look really legit and would appear to come from an invitation company like punchbowl. They will often feature a real name of a friend or church attender and will actually come from a legitimate email address. When you click on the link to open or accept the invitation, the site will ask you for your email address and password.

Here are some ways you can recognize these malicious emails:

- Look carefully at the sender. It is easy to spoof the name that appears before an email, but much harder to actually spoof the email address. For instance, a recent spoof email came from "Pastor Aaron Henning <churchofficeonline888@gmail.com>". **Communication from the church will always come from an official church email address [@scalliancechurch.com](mailto:scalliancechurch.com).**
- Look for any unusual requests in the email, especially online bank transfers or gift cards. **All giving to the church should be done through official channels like scalliancechurch.com/give, via mail (1221 W. Whitehall Road) or the onsite dropboxes.**
- Be careful if a link from an email is ever asking for personal information like your email password, Social Security Number, or banking information. **The church will never need any of this information and will never ask for it.**

What do I do if I get an email that looks suspicious?

1. Don't follow any links in the email or reply to it.
2. If you have a suspicious email coming from the church, forward it to me at bill@scalliancechurch.com so I can make sure none of our systems have been compromised.
3. Flag the email as "Scam" or "Phishing" through your email client. This looks different on each email service.
4. Delete the email so you don't accidentally do anything with it later.

Please don't hesitate to reach out to me or call the office if we can help you sort through any suspicious emails claiming to be from the church.

Sincerely,

Bill Jester
State College Alliance Church IT Director