# Financial Responsibility Agreement

Jane Doe <jane.doe@mail.gvsu.edu>

John Smith

According to our records, you or an SIU administrator on your behalf processed at least one registration transaction within the last week. As a result of this transaction you are receiving an email reminder of the terms and conditions of the Southern Illinois University Financial Responsibility Agreement that you previously accepted or was accepted on your behalf.

Click here to review the agreement: MySIU

This email does not require any response or action. However, you can reply to: grantaid@siu.edu if you have questions about the Financial Responsibility Agreement.

Thank you,
Office of the Bursar

---

## Signs of a Questionable Email

1. **Look carefully at who the email is from.** Look at the email address itself; Southern Illinois University will not send an email from @mail.gvsu.edu. If the address does look correct, check the spelling. Is SIU actually S1U or S!U?

2. **Pay attention to the subject line.** If an email is coming from a trusted person or company, ask yourself if the subject line is typical based on what they normally send. Does it have urgent wording? Are there typos? If something seems wrong, it probably is.

3. **Look for external email alerts.** Any email sent to an SIU account from an outside organization has red text at the top stating that it is from an external source. If you see this red headline, take a close look at the email before you do anything or respond to the sender.

4. **Don’t always trust a logo.** If a logo is on the internet, anyone can find it and use it. Although logos can be reassuring, you should not immediately trust an email just because it has a logo.

5. **Be wary of typos, poor grammar, or odd phrasing and sentence structure.** Although logos can be reassuring, phishing emails are notorious for typos and poor grammar. Ask yourself if the email sounds like the person or company supposedly sending it. If you are in doubt, you can always call and verify that the sender did send you the email.

6. **Avoid links and attachments.** Unless you are expecting an email with a link or attachment in it, avoid clicking on or opening them. To screen links and attachments, hover your mouse above a link and look at the URL that appears in the bottom left corner of your screen. If the email claims to be from SIU, but is taking you to a website called fluffysaluki.com, it is probably a scam.

---

**When in doubt...**

Contact SalukiTech at 618/453-5155 or salukitech@siu.edu to ask them to help you vet the email. You can also click on the Report Message button in the top right corner of Outlook.