Spam & Phishing Email Warning
March 15, 2026

OUUF members and friends are regularly receiving phishing emails. The latest example asks recipients to **forward a copy of our fellowship roster**, which should never be shared by email.

These messages are often made to look like they come from someone you know, but they are attempts to obtain personal information.

If you receive an email that seems unusual, requests private information, or asks you to send documents or contact lists, **please do not respond or click any links**.

A few reminders to help protect yourself and the fellowship:

- **Do not share the OUUF roster or personal contact information by email.**
- **Check the sender's email address carefully**—phishing emails often use addresses that look similar but are slightly different.
- **Be cautious of urgent requests** or messages asking for favors, money, or sensitive information.
- **When in doubt, verify** by contacting the person directly through a known phone number

---

Spam and phishing emails are becoming more common and often look like they come from trusted organizations, businesses, or even people you know. These messages are designed to trick you into giving away personal information, passwords, or financial details.

Common Signs of Phishing Emails

Be cautious if an email:

- Urges you to act **immediately** or threatens account closure.
- Asks for **passwords, Social Security numbers, banking information, or payment details**.
- Contains **unexpected attachments or links**.
- Has a **sender address that looks unusual or slightly misspelled**.
- Includes **poor spelling or grammar**.
- Claims you have **won a prize or refund you did not request**.

How to Protect Yourself

- **Do not click links** in suspicious emails. Instead, go directly to the organization's official website.
- **Do not open attachments** unless you are certain of the sender.
- **Check the sender's email address carefully.**
- **Hover your mouse over links** to see the real destination before clicking.
- **Use strong passwords** and consider a password manager.
- **Enable two-factor authentication** whenever possible.
- **Keep your computer and antivirus software updated.**

What To Do If You Receive a Suspicious Email

- **Do not reply** to the email.
- **Delete it** or mark it as spam.
- If it appears to be from a company you use, **contact the company directly** using their official website or phone number.
- If you think you clicked a malicious link, **change your passwords immediately** and run a virus scan.

Remember

Legitimate organizations **will not ask for sensitive information by email**.

Staying cautious and verifying unexpected messages can help protect your personal information and prevent fraud.