SEATTLE UNIVERSITY

How to Avoid Common Email Scams

Hi Rudy,

While you are becoming accustomed to using your SeattleU email, be aware of phishing emails that may be sent to you from other seattleu.edu email addresses or emails claiming to be from representatives of Seattle University.

Phishing attacks can have serious security implications for both individuals and the institution as a whole. **Seattle University will never send links to reset a student account or password nor demand you act immediately without providing specific deadlines.** It is common for phishing emails to claim your student account will be deactivated unless you click on a link or provide sensitive information, such as your login information.

If you suspect you may have engaged with a phishing email, don't panic, call the Seattle University Service Desk so they can help reset your password at 206 - 296 - 5571. Be prepared with your SU ID for verification.

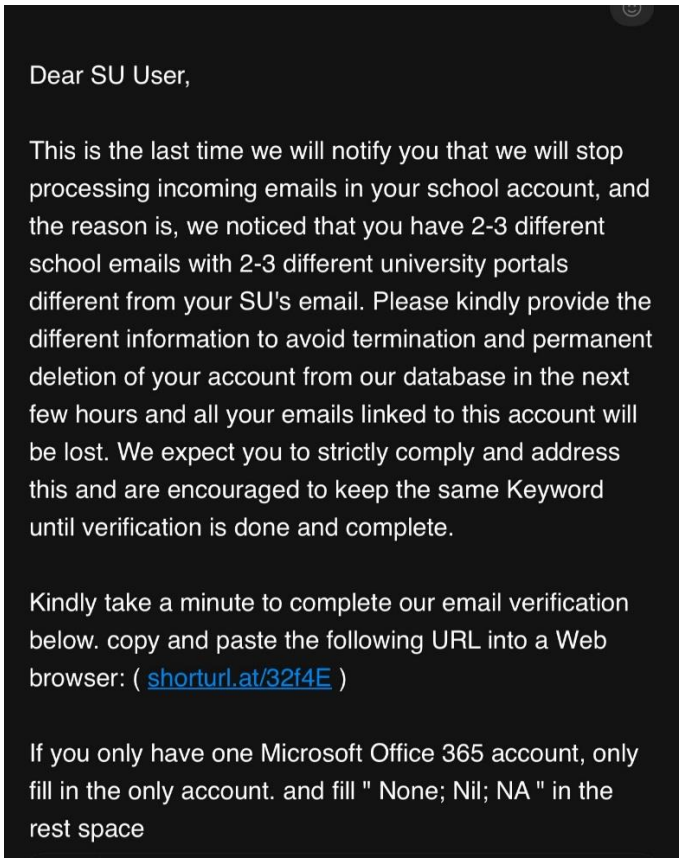
To safeguard our university's resources and personal information, we kindly ask for your cooperation in taking the following precautions:

1. **Stay Vigilant:** Be cautious when receiving unsolicited emails, especially those requesting payment, sensitive information, or indicating a sense of urgency which require immediate action. *Verify the sender's email address and look for any inconsistencies or unusual elements*. Be cautious of anything coming from an unfamiliar sender.
    - *If you are viewing the email on a mobile device***:** Mobile email apps often only show the display name by default. Please make sure you are viewing the originating email address.
2. **Verify Requests:** If you receive an email requesting personal information, your student account information, or financial information, **confirm the legitimacy of the request by reaching out to the supposed sender *using contact information from an official source, not from the email itself*.**
    - *Internal accounts can become compromised*. If someone you know suddenly asks to send payment to a new bank account number, address, or unfamiliar company, we highly recommend calling the requester *using contact information from an official source, not from the email itself.*
3. **Double-Check URLs:** Hover your mouse over any links in the email to preview the destination URL before clicking. Ensure that the URL matches the official website and does not lead to a suspicious or unknown site.
4. **Don't Share Sensitive Information:** Never share personal, financial, or login information via email. Legitimate organizations will not ask for such information through email.

5. **Report Suspicious Emails:** If you encounter an email that seems suspicious, do not engage with it. **Instead, report it to our Information Security team using the Report Message button in outlook.**
6. **Educate Yourself:** Familiarize yourself with common phishing tactics, so you can recognize and respond to potential threats effectively.

   To read Seattle University articles about phishing emails, you'll need to login to your Seattle University credentials (email and password) then you can read the phishing page at the SeattleU website.

Here is an example of a phishing email:



Dear SU User,

This is the last time we will notify you that we will stop processing incoming emails in your school account, and the reason is, we noticed that you have 2-3 different school emails with 2-3 different university portals different from your SU's email. Please kindly provide the different information to avoid termination and permanent deletion of your account from our database in the next few hours and all your emails linked to this account will be lost. We expect you to strictly comply and address this and are encouraged to keep the same Keyword until verification is done and complete.

Kindly take a minute to complete our email verification below. copy and paste the following URL into a Web browser: (shorturl.at/32f4E)

If you only have one Microsoft Office 365 account, only fill in the only account. and fill " None; Nil; NA " in the rest space

If you have any concerns or questions regarding email security or phishing prevention, please do not hesitate to contact the Service Desk at (206) 296-5571 or servicedesk@seattleu.edu for support.

Thank you for your attention to this matter.

Orientation Programs | SEATTLE UNIVERSITY
901 12th Avenue, Seattle, WA 98122-1090
Office: (206) 296-2525