Holiday Scams

MONTCLAIR STATE UNIVERSITY | Information Security

Stay safe during the holiday season by watching for these common scams.

Remember: If you receive a suspicious message, use the **Phish Alert Button (PAB)** to report.

1. Fake Package & Mailroom Alerts

Attackers impersonate:

- Campus mail services
- Amazon, UPS, FedEx, USPS

They claim your package is delayed or needs verification.
Goal: Steal your University login or personal info.

2. Holiday Travel Update Scams

Common for students and employees traveling home:

- Fake flight cancellations
- “Confirm your booking” messages
- Bogus hotel/Airbnb issues

Goal: Capture travel logins or payment info.

3. Fake HR, Registrar, or Department Emails

Scammers pose as University departments and send:

- “Check your adjusted holiday schedule”
- “Update payroll before processing”
- “Verify student records before break”

Goal: Get you to enter Montclair credentials on a fake site.

4. Holiday Giving & Charity Scams

Fraudsters send messages about:

- Fake food drives
- “Urgent” holiday fundraisers
- Bogus student-organization charity events

Goal: Steal money or financial information.

5. Impersonation of Faculty, Staff, or Supervisors

Around holidays, gift card scams spike:

- “I need gift cards for a holiday event—can you buy them?”
- “Text me the codes; I’m in a meeting.”

Goal: Immediate financial loss.

6. Holiday-Themed Social Engineering

Friendly-looking but dangerous messages:

- “Photos from last year’s holiday party—click to view”
- “Is this you in this video?”
- Holiday e-cards

Goal: Spread malware or harvest passwords.

7. Fake Store Discounts or ‘Student Deals’

Scammers know students are shopping Black Friday sales. They send links to:

- “Exclusive student discounts”
- “Campus partner promotions”

Goal: Steal payment info or install malware.

8. Bogus Scholarships or Financial Aid Alerts

Scammers send:

- “Emergency grants available before the holidays”
- “Apply now for end-of-semester financial assistance”

Goal: Gather sensitive personal and financial information.

9. Fake Montclair Account Lockout Notices

Common subject lines:

- “Your account will deactivate for the holiday”
- “Verify your Duo/MFA before break”
- “Password expires today”

Goal: Trick you into entering your login info.

10. Fake Giveaways of Items or Equipment

Scammers impersonate students, staff, or campus groups to offer “free” items such as:

- Pianos or instruments
- Dorm furniture
- Electronics or school merch
- “Unclaimed” department equipment

They often claim the item is available if you “just pay the delivery fee.”
Goal: Collect money, personal info, or get you to click malicious links.