
Spotting Fake Amazon Emails

A Quick Reference Guide for University at Buffalo End Users

■ How to Spot a Fake Amazon Email

Phishing emails impersonating Amazon are common across all industries. They are **not** related to your UB Amazon Business account — scammers send these to publicly available email addresses. Here are the red flags:

X Suspicious sender address — Real Amazon emails come from @amazon.com. Fakes use random addresses like *qodoha-fizuxa@outlook.com* or misspelled domains.

X Urgency or threats — "Your account will be suspended" or "Verify immediately" language designed to panic you into clicking.

X Asks you to call a phone number — Amazon will never include a phone number in an email and ask you to call to verify a purchase.

X Fake invoice or order you didn't place — If you didn't order it, it's not real. Don't click "View Order" or "Cancel Order" buttons.

X Generic greeting — "Dear Customer" instead of your actual name or organization.

✓ What Legitimate Amazon Business Emails Look Like

When Amazon communicates with you, here's what to expect:

✓ **Sender is @amazon.com** — Authentic emails come from recognized Amazon domains and display the Amazon smile logo icon in Gmail, Yahoo, and other major providers.

✓ **References orders visible in your portal** — Any real order confirmation or account notification corresponds to activity you can see at business.amazon.com.

✓ **Never asks for sensitive info via email** — Amazon will never ask you to share passwords, payment details, or Social Security numbers by email or phone.

✓ **No pressure to act immediately** — Legitimate communications don't threaten account suspension or demand you call a number within minutes.

■ What To Do

If you receive a suspicious email that appears to be from Amazon:

- 1. Don't click, don't call.** Do not click any links, open attachments, or call any phone numbers in the email.
- 2. Verify in the portal.** Go directly to business.amazon.com and check your order history. If there's no matching order, the email is fake.
- 3. Report it.** Forward the suspicious email to **stop-spoofing@amazon.com**. This helps Amazon's security team take down phishing sites — often within hours.

■ **The golden rule: If you didn't place an order, there's nothing to verify. Just delete it.**

Amazon took down 70,000+ phishing websites and 14,000 fraudulent phone numbers in 2025. This effort is ongoing and automated.
Report suspicious emails: stop-spoofing@amazon.com | Verify orders: business.amazon.com

Prepared by your Amazon Business team • June 2026