BETHEL COLLEGE
INFORMATION AND MEDIA SERVICES

How to Recognize and Report Phishing Emails

A guide for students, faculty, and staff

What is Phishing?

Phishing is a type of cyberattack where someone impersonates a trusted person or organization — like IT, your bank, or a colleague — to trick you into revealing passwords, clicking malicious links, or transferring money.

Phishing emails are the most common way that accounts get compromised. Recognizing them is one of the most important digital safety skills you can have.

Red Flags: What to Look For

No single sign guarantees an email is phishing, but the following are common warning signs. The more of these that appear together, the more suspicious you should be.

Red flag	What it looks like
Urgency or threats	Language like "Your account will be suspended in 24 hours" or "Immediate action required" is designed to panic you into acting without thinking.
Mismatched sender address	The display name looks right ("IT Help Desk") but the actual email address is something like helpdesk@random-domain.com or a misspelling of your school's domain.
Suspicious links	Hover over any link before clicking. If the URL doesn't match where it claims to go, or uses a shortened URL (bit.ly, tinyurl), treat it as suspicious.
Requests for credentials	Legitimate IT staff will never ask for your password, MFA code, or security questions by email. Ever.
Unexpected attachments	An unsolicited attachment — especially .zip, .exe, .docm, or even .pdf files — can contain malware. Be cautious even from known senders if the email is unexpected.

BETHEL COLLEGE
INFORMATION AND MEDIA SERVICES

Red flag	What it looks like
Generic greetings	"Dear user" or "Dear student" instead of your name can indicate a mass phishing campaign.
Poor grammar or unusual tone	Awkward phrasing, odd capitalization, or a writing style inconsistent with the supposed sender.
Unexpected requests for money or gift cards	Requests to purchase gift cards and share the codes, or to urgently transfer funds, are almost always scams — regardless of who the email appears to be from.

Common Scams at Our Institution

These are the types of phishing most commonly seen in college environments. Knowing what they look like makes them much easier to spot.

⚠ Fake IT / Help Desk Emails

Common targets: Everyone — students, faculty, and staff

- Sender appears to be from IT, the Help Desk, or a system administrator
- Claims your account has been locked, compromised, or will expire
- Asks you to verify your credentials by clicking a link or replying with your password
- May reference real systems your school uses (Google, Microsoft, Banner, etc.) to appear credible
- Legitimate IT staff will never ask for your password or MFA code by email

Example: *"Your school email account has exceeded its storage limit. Click here within 48 hours to verify your account or it will be suspended."*

⚠ Financial Scams (Fake Invoices & Wire Transfer Requests)

Common targets: Faculty, staff, and anyone with financial responsibilities

- Impersonates a vendor, senior administrator, or colleague
- Requests an urgent wire transfer, ACH change, or payment to a new account
- May reference a real project or vendor name to seem legitimate
- Often sent from a lookalike domain (e.g. school-edu.com instead of school.edu)

- Always verify financial requests through a separate, known communication channel — not by replying to the email

Example: *"Hi, I'm in a meeting and need you to process an urgent payment to a new vendor. I'll explain later — please handle ASAP."*

⚠ Job Scams

Common targets: Students, particularly those actively job-searching

- Offers an unusually well-paid, flexible, or easy job (e.g. "personal assistant," "remote data entry")
- May appear to come from a faculty member, department, or campus employer
- Quickly moves to asking for personal information, a bank account number for "direct deposit," or to cash a check
- Check-cashing scams: you receive a check, deposit it, send money back — the check later bounces and you're liable
- Legitimate campus employers post jobs through official channels; they will not email you out of the blue

Example: *"A professor has recommended you for a part-time research assistant role paying $500/week. No experience needed. Reply to get started."*

What to Do If You Receive a Suspicious Email

1 **Do not click any links or open attachments**
Even if the email looks legitimate. If you are unsure, navigate directly to the website by typing the address yourself rather than clicking a link in the email.

2 **Do not reply or provide any information**
Do not enter your username, password, or MFA code on any page you reached by clicking a link in a suspicious email.

3 **Report it**
In Gmail, click the three-dot menu and then choose "Download message". This will download a .eml file. Send that as an attachment to phishing@bethelks.edu so we can be aware of trending

BETHEL COLLEGE
INFORMATION AND MEDIA SERVICES

cyber threats on campus. Also, it is advisable to use Gmail's built-in "Report phishing" option (three-dot menu → Report phishing).

4 **Delete the email**
Once reported, delete it from your inbox and empty your trash.

5 **If you already clicked a link or entered credentials…**
Change your password immediately and contact the IMS Help Desk right away. The sooner you act, the better the outcome.

Quick Reference: Phishing Checklist

If you receive an unexpected email, run through this checklist before taking any action:

- ☐ Do I recognize the sender's email address (not just the display name)?
- ☐ Was I expecting this email?
- ☐ Does the request make sense for this person to be asking by email?
- ☐ Does the email create urgency, pressure, or threats?
- ☐ Does it ask for credentials, personal info, money, or gift cards?
- ☐ If there is a link, does the URL match the claimed destination when I hover over it?
- ☐ If there is an attachment, was I expecting it?

If you answered "no" or "I'm not sure" to any of these questions: do not click, do not reply, and report it to IT.

Questions? Contact the IMS Help Desk.

If you receive a suspicious email and are not sure what to do, contact the IMS Help Desk before taking any action.

If you have already clicked a link or entered your credentials, contact us immediately — we can help minimize the impact.