How to Spot a Phish

Phishing emails and texts try to trick you — here's how to catch them before they catch you!

MONTCLAIR STATE UNIVERSITY | Information Security

🚩 Top Red Flags of a Phishing Message

1. Urgent Language

"Act now or your account will be disabled!"
⚠️ Scammers create panic to make you click without thinking.

2. Suspicious Links or Attachments

Hover before you click — does the link look weird?
🛑 Never open attachments from unknown senders.

3. Generic Greeting

"Dear user" or "Hello customer"
✉️ Legitimate messages usually use your real name or NetID.

4. Unexpected Requests for Info

"Confirm your password," "Send your SSN," "We need your login to verify."
🔐 Legit senders will *never* ask for passwords or sensitive data over email.

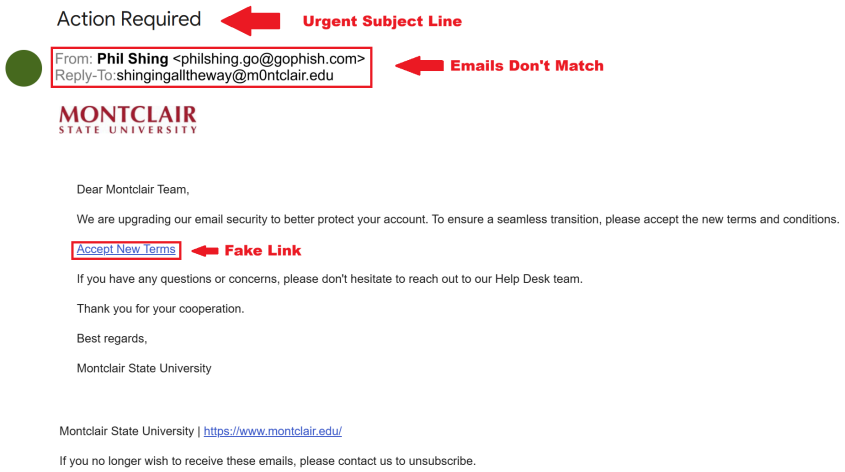
5. Email Address Doesn't Match the Sender

Example: support@m0ntc1air.com
🔍 Always double-check the sender's email — look for subtle misspellings or extra characters.

6. Offers Too Good to Be True

"You won a free iPad!" or "Get paid $500 a week for remote work!"
💸 If it seems too good to be true, it probably is.

🐟Real Phish Example (Visual Section)



🛡️ What to Do if You Suspect a Phish

1. **Don't click anything — no links, no downloads**
2. **Don't reply — even to say "Is this legit?"**
3. **Report it using the PAB or forward it to phishfiles@montclair.edu**
4. **Delete the message**

✅ Pro Tips

- **Use MFA on all your accounts (including personal!)**
- **Use a password manager (1Password or LastPass are great!)**
- **When in doubt, use the PAB or forward it to phishfiles@montclair.edu**