

# Phishing email analysis



Hepatitis A Case Reported – Please Review.eml  
File

Is this a phishing email and why?

Yes — this email strongly appears to be a **phishing attempt**. Here's why:

## 1. Unusual Sender Chain

- The original message claims to be from *Ace Evans @evergreen.edu* (Evergreen State College) but was inexplicably sent to a *University of Maine* professor.
- The UMaine staff [REDACTED] even notes in the thread: *"I don't have a clue why I am receiving this message from Evergreen State College."* This mismatch is a red flag.


## 2. Suspicious Link

- The forwarded "Hepatitis A Case Reported" notice instructs recipients to click a link to a *Health Service Center*.
- The link is not a clear Evergreen or UMaine domain — it's embedded as a generic "Health Service Center" hyperlink, a common phishing tactic to hide a malicious URL behind a trustworthy-looking phrase.

## 3. Exploiting Urgency and Fear

- The subject line references a **serious health alert** ("Hepatitis A Case Reported") to push recipients into clicking quickly without thinking. Fear-based hooks are classic phishing methods.

## 4. Legitimacy vs. Context Conflict

- Technical checks (SPF, DKIM, DMARC) appear to pass for **maine.edu** , but that only shows the email wasn't spoofed at the SMTP layer — not that the content is legitimate. Phishers sometimes compromise a real account or abuse forwarding to add credibility.

## 5. No Official Distribution Method

- Legitimate university health alerts would usually come directly from the institution's Health Services or Communications office, not via a forwarded chain from an unrelated school.

## ✓ Conclusion:

This email is **malicious** — a phishing attempt designed to lure recipients into clicking the disguised "Health Service Center" link. Even though it passed authentication checks, the mismatched context, forwarding confusion, and suspicious embedded link are clear warning signs.

Do you want me to draft a **warning notice** you can send to your colleagues/students about this phishing campaign?

## Sources