



## Phishing

### RECOGNIZE PHISHING SCAMS

1. The sender's address is in a different format than the rest of the organization's (e.g., all emails within the organization follow the format of "firstname.lastname@county.gov" but the message claiming to be from someone within the organization is different).
2. There are frequent misspellings and poor grammar. Many attacks originate in non-English speaking parts of the world.
3. The message asks users to click on links or open attachments.
4. It sounds too good or too bad to be true (e.g., "Claim your tax return now" or "We have your kids.")
5. The message includes outrageous or sensational headlines or imagery that entices you to click on them.

Inbox 14  
Drafts  
Sent Items  
Deleted Items  
Junk Email [1] 6  
Outbox  
RSS Feeds  
Search Folders

Reply Reply All Forward  
Mon 9/23/2024 2:30 PM  
Mark Williams <m.williams@minncounty.net> 1  
RE: Late Invoice - PLEASE PAY! 5  
To Michael Peterson

Attached Invoice.html 72 KB

Accounting: 7  
Your account is severely past due. 2  
Click attached to view invoice. 3  
Please pay promptly before legal action is taken. 4  
Sign in to customer portal to pay now.  
Thank you, Customer Service  
[https://pay-sense-us.me/azvkypkip/titan\\_ma\\_grey/](https://pay-sense-us.me/azvkypkip/titan_ma_grey/) 8  
Click or tap to follow link.

6. The message is in a spam or junk email folder. Many IT departments and email providers have filters that automatically screen spam messages. If a message is in the spam folder, it can be a clue that it may not be legitimate.
7. There is a vague greeting and sender. Often bulk phishing attempts are not directed to individual people. Messages may

start with "attention" or another generic word or phrase. Similarly, messages that end with a title or vague location should be viewed with suspicion (e.g., "web administrator" or "help desk").

8. Hovering the mouse cursor over the link shows a different Web address than the indicated link.

### PREVENTION

If a message has one or more of the elements above, you should:

- Contact IT and follow their directions.
- Forward any requests for private information to the responsible authority for your organization.
- Do not open the message, click on any links or items or follow instructions in the message, such as sending confidential information or passwords.

### NOTES: