CASE WESTERN RESERVE UNIVERSITY EST. 1826
think beyond the possible

Google Mail Reference Sheet
Managing Spam

CWRU Google mail has a standard set of filters that determine if mail is legitimate or most likely spam. Spam can still enter your inbox, and legitimate mail may still be labeled spam.

To ensure that email is handled correctly, spam management must be conducted in CWRU Google webmail, not a client such as Outlook or Thunderbird. Go to http://webmail.case.edu to manage spam settings.

To report spam – Click the check box next to the spam email and then click the **Report Spam** button. The message will disappear from your inbox, and any messages received in the future from that address will automatically be sent to the Spam link. You can find messages marked as spam by going to the Spam link on the left side of the page.

To remove legitimate mail from spam – Click the Spam link on the left side of the screen. Click the checkbox next to the item that is not spam and then click the **Not Spam** button. The message will move to your Inbox, and any messages received in the future from that address will also appear in your Inbox.

To delete all spam messages – Click the Spam link on the left side of the screen. Click the delete all spam messages link above the first message. Spam is also deleted automatically after 30 days.

Phishing – Phishing is a type of spam. It is the fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an email. Phishing emails that masquerade as a CWRU authority tend to urge recipients to click on a link in order to keep their accounts open. These links take users to official-looking but fraudulent imitations of the CWRU Single Sign-On page, hosted on non-CWRU-owned web servers. While CWRU Information Technology Services (ITS) *does* send notifications to users when passwords need to be changed to comply with the 365-day password age policy, those notification emails intentionally contain no links. You should NEVER enter your CWRU account credentials into a page outside the *case.edu* domain.

Detecting a phishing attempt – Any email that requests private information such as a username, password or pin, social security number, credit card or bank account number, is probably an attempt to phish. If you suspect that you have received a phishing email, do not respond to it or click on any links it contains. Use the **Report Spam** button to move the email to the Spam link.

If you have additional questions about phishing, please contact the ITS Help Desk (216) 368-HELP (4357).