

Google Mail - Spam Filtering

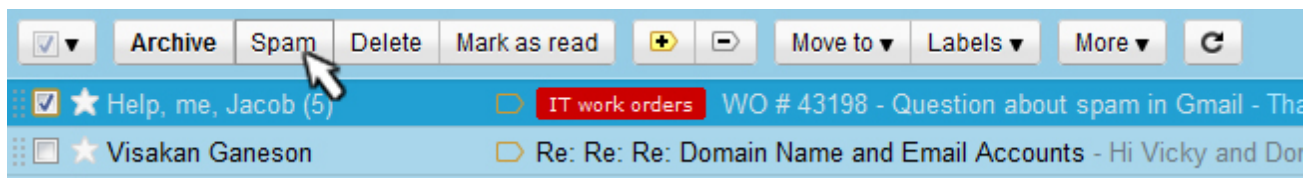


Google has very good spam filters, and Everett Community College also applies further spam filters to incoming email. This will catch most spam, but no filtering system is 100%. Because of this, you may still receive malicious messages and you need to be cautious.

Common Spam

One of the most common ways that spam can get through a spam filter is if it comes from a legitimate user that has had their **account compromised**. This allows a spammer to log in as that user to their web mail and send any email they want.

When a spam filter looks at an email to decide if it is legitimate, the content of the message is only one of the things that it looks at. Looking at factors other than the content is a major way to detect spam. In fact, the actual content of the message is a low-weighted indicator of spam, and other factors such as a **valid message source** can outweigh it.



Because no filter can block all spam, it is important that you look for typical types of spam coming in to your inbox and mark them with the **spam button** as shown above. This helps the spam filter to recognize other emails that are similar or from that same address and block them.

For example, emails with any of these features should be considered questionable:

- no subject title
- a generic title that you did not originate, such as “The file you requested”
- instructions to validate your account settings through a hyperlink
- a request for any kind of verification, password, or id
- from someone you don’t know about a subject that you didn’t originate

The IT Department will never email a request for you to provide a password or id or verify an account by clicking on a link. Any software that is installed by IT would also never send an email asking for your password or id.

Consider any email that requests a password, ID code, or verification of an account as spam and please report the email to Help Desk.