When to Suspect:

Urgency & Warnings:

Many of these scams are designed to manipulate the target's emotions and fears. They use language that conveys a sense of urgency where victims are made to fear losing something important, or feel the temptation to gain something. Eg. "Your email has been accessed by a third party. Please login immediately & change your password." or "I just transferred you $1,000.00. Please login and verify this transaction."

Every Thief Leaves a Clue!

Look for spelling errors, bad grammar, or slightly altered logos. If anything in the email looks unusual or suspicious to you, your instincts may be right. Also, check the email address (banks never send emails from a Gmail or Yahoo domain). Hover your mouse over the link (but don't click!) to see if the link will take you to a legitimate website.

Generic Greetings

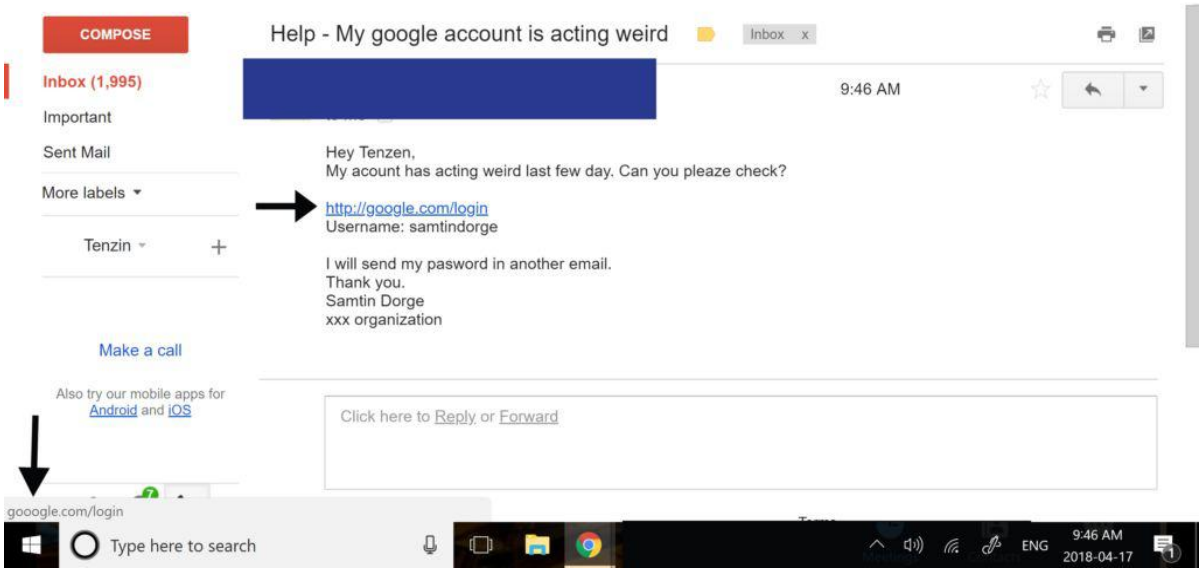
Most common scams may not be personalized. Emails may be generic and addressed in general terms such as, "Dear valued customer,". That said, we also have to be mindful that targeted phishing attacks can be personal, "Dear Tenzin," etc. If you are not expecting any communication from a group or an individual, do not open the email and always confirm the sender of suspicious emails through text or phone.

How to respond:

- Do not open attachments
- Do not open links
- Do not reply
- Do not enter any information
- Block and Delete

Protect yourself:

1. Always double check the website address before you enter your email ID and password.



2. Change your passwords every few months.
3. Use different password for different accounts.
4. Always use 2-Step Verification.
5. Install Password Alert extension in your Google Chrome browser. It protects you against phishing attacks.
6. Don't Wait! Update your operating system and software today.