Signs of a compromised email

Have your account settings been changed?

Critical account settings such as your recovery email, phone number and multi-factor authentication options shouldn't be changed by anyone but you.

Are there emails in your sent folder that you didn't send?

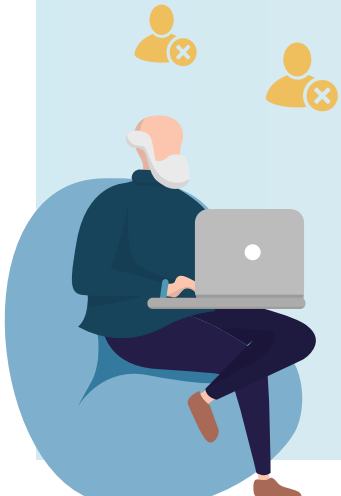
If you didn't send the emails in your sent folder, then someone else may have.

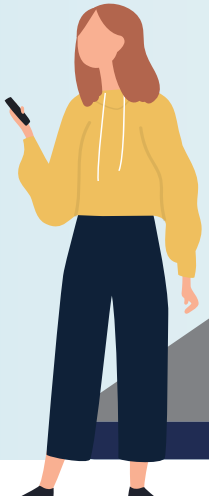
Have you received password change requests of confirmations?

Unrequested password change emails can indicate that someone is trying to figure out which sites you use to try and get control of your accounts.

Have your contacts noticed something odd?

If someone has hacked your email account and has been sending out strange emails, you may start hearing about it.





Have you noticed logins to your account from unfamiliar IP addresses or locations?

Your email provider should let you view the login history for your account. If your email has been compromised, then you may see your email being accessed from other locations that you haven't been.

Are you locked out of your email?

After obtaining control, hackers may change your email password to prevent you from getting back in.