Investigate the Display Name/Email Address:
Changing the “From” name is a classic phishing ploy for hackers, known as Spoofing.
Make sure the name and email address make sense.

Spelling Mistakes:
Legitimate emails rarely have major spelling mistakes or poor grammar – brands and corporations wouldn’t allow that. Can you catch the typos?

From: Jobandinternshipfair <beygivens.w@gmail.com>
Sent: Monday, September 23,201910:28AM
To: Xxxxx Xxxxx; Yyyyy Yyyyyy; Zzzzz Zzzzz
Subject: Part Time Job Fair, Monday September 23rd

Review the Salutation:
Is the salutation to a vague "Valued Customer?" or “Dear User”? Legitimate businesses will often use your first and last name, so beware if it doesn’t.

Good Morning! Hope you’re enjoying you summer.

Seeking a job or internship this fall? Mark you calendar- the UNICEF Fall Part Time Job and Internship Fair is coming up September! This is the perfect opportunity to connect with both on and off campus employers seeking ALL majors to fill part-time and internship positions!

If you looking http://www.badguys-hq.xyz Ctrl+Click to follow link please (see attached). If you want to register, go to our website at https://www.unicef-jobs.org

Act soon since we fill up fast!!!

Feel free to pass along the application to anyone that maybe a good candidate.

Best, Terry

Attachments can be Dangerous Too!
Hackers can embed attachments with viruses and malware that can steal your passwords, damage files on your computer, or even spy on you.

The Signature Line
Are you able to contact the company? Does the email provide details about the signer? Legitimate businesses always provide contact information.

Look But Don’t Click
Hackers love to embed malicious links with fake link text. To expose this fraud, hover your mouse over the link.

Urgent or Threatening Language
Beware of emails that promote a sense of urgency or fear. Hackers know people will act without thinking if they feel rushed.