Email Security Tips

1. **Carefully Review Email Content**: Pay close attention to the email's content. Be cautious if the sender asks you to contact them privately instead of via email.

2. **Identify Low-Level Scams**: Scams often initially request action without specifying details in the email e.g. can you help me with something?

3. **Managerial Pressure**: Scammers will sometimes check sources like LinkedIn or the company website to see who has authority then make suspicious requests of their team.

4. **Beware of Spoofed Emails**: Hackers may spoof legitimate emails to appear as if they are from someone you know.

5. **Handle Sensitive Data with Caution**: If asked for sensitive information, be on high alert. Verify the request by contacting the sender through a separate email or, preferably, a phone call. Do not use the phone number provided in a suspicious email's signature.

6. **Do Not Interact with Suspicious Emails**: Do not reply or click any links. Notify us immediately if you find an email suspicious.

7. **Monitor Unrecognized CC'ed Mailboxes**: Keep an eye out for unfamiliar email addresses in the CC field.

8. **Verify Sender's Email Address**: Double-check the sender's email address, as it may not match the person they are impersonating.

9. **Block Suspicious Email Addresses**: In Outlook, right-click the email in the list, go to Junk, and select Block Sender.

10. **Spam Filter Settings**: Your spam filter is set to low. We do not recommend increasing it, as it may classify many external collaborators' emails as spam, especially if they send frequent emails.

11. **When in Doubt, Contact Us**: If you are unsure about any email you receive, do not hesitate to call us for verification before interacting with it. It is better to be safe than sorry.