How to Handle SUSPICIOUS EMAILS

If you don't correctly handle a suspicious email, you could fall victim to a phishing attack.

DON'T REPLY TO THE EMAIL

If you reply to the email, you may increase the security risk. You could actually be communicating with a cybercriminal.

DON'T FORWARD THE EMAIL

Never click a link or open an attachment that you were not expecting. If you open a suspicious image attachment, the file may actually open an installation window. Or, if you click a malicious link, the link may redirect you to a fake login page. If you forward a phishing email, you increase the risk of a security breach because your coworker may click the phishing link as well.

REPORT THE EMAIL

The best way to handle a suspicious email is to report it to IT. The IT team will assess and mitigate the threat. Ways to Report: Create a a Mojo Helpdesk ticket. If you're not sure how, ask a manager or supervisor for help. You can also call (670) 322-1238 or email *tech.support@cnmipss.org*.

Handling suspicious emails properly is crucial for protecting our information and school networks.