12 Tell-Tale Signs of Phishing Emails

Cybersecurity is everyone's responsibility.

1 SUSPICIOUS SENDER ADDRESS

Check the email address exactly matches the organization it claims to be from.

2 MISMATCHED URLS

Hover over links to see if the URL matches the expected destination.

3 GENERIC GREETINGS

Look out for generic greetings like "Dear Customer" instead of your name.

4 UNUSUAL FORMATTING

Look for inconsistencies in email formatting or design.

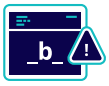
5 URGENT OR THREATENING LANGUAGE

Be wary of emails urging immediate action or threatening consequences.

6 TOO GOOD TO BE TRUE OFFERS

Be skeptical of offers that seem too good to be true.

7 SPELLING AND GRAMMAR ERRORS



Notice poor grammar or spelling mistakes, which are uncommon in official communications.

8 CHECK THE SIGNATURE

Verify if the email signature matches the company's standard format.

9 UNFAMILIAR LINKS OR ATTACHMENTS

Avoid clicking on unfamiliar links or downloading attachments.

10 CROSS-VERIFICATION

If in doubt, contact the sender directly through official channels to verify the email's authenticity.

11 REQUEST FOR PERSONAL INFORMATION

Legitimate companies rarely ask for sensitive information via email.

12 ASKING FOR MONEY OR PAYMENTS

Be cautious if the email asks for money, especially via untraceable methods.

Any questions, please contact _____

TRUEFORT