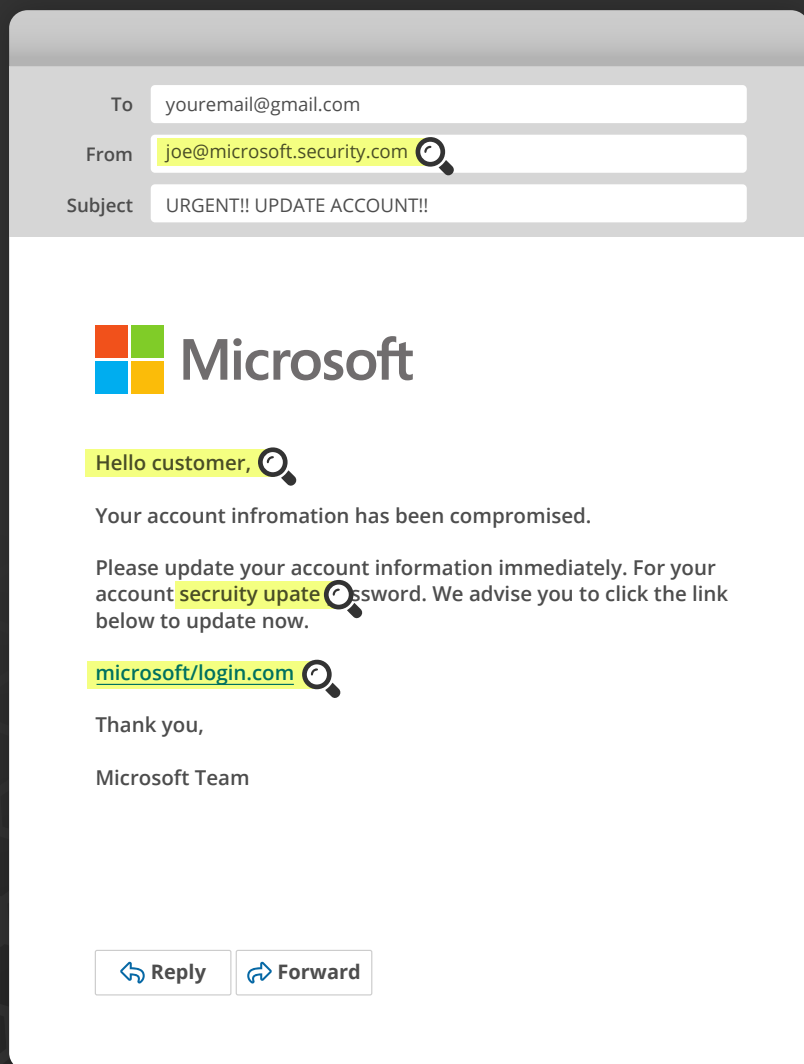


BEWARE OF BUSINESS EMAIL COMPROMISE



Business Email Compromise (BEC) is a cyberattack where attackers impersonate trusted individuals or organizations through emails to deceive victims into taking actions, such as transferring funds or sharing sensitive information.

RECOGNIZING A BEC ATTACK

- Poor spelling, grammar and punctuation**
BEC attempts often contain errors in language usage.
- Unusual formatting, appearance or domain**
Be cautious of messages that look different from the sender's typical style or come from random domains.
- Non-official email address**
Messages not originating from official email addresses or domains may indicate a BEC attack.
- Improper greeting or signature**
Unusual greetings, signatures or contact information could suggest phishing attempts and BEC attacks.
- Unusual fund requests**
Payment requests to uncommon addresses through unusual methods should be treated cautiously.

X Email-only communication

If the sender avoids other channels of communication, it's suspicious.

X Urgency & rushed transactions

BEC attackers create a sense of urgency to manipulate victims into acting hastily.

X Unusual fund requests

Payment requests to uncommon addresses through unusual methods should be treated cautiously.

ACT NOW TO PROTECT YOUR INBOX

We help you combat advanced cyberattacks with ongoing awareness training.



651-448-9900 | www.bomberjacket.net
3260 163rd LN NW Greater Minneapolis-St. Paul Area,
Minnesota 55304