During the exercise, I analyzed three phishing examples and one real email from my spam folder.

The first fake message claimed to be from a delivery service (postapaket.xyz) and asked me to confirm my details within 24 hours, the link led to a suspicious .ru domain.

The second message pretended to be from a bank (bankaa-si.com) and warned that my account would be deactivated. The sender domain and link were fake.

The third message offered a prize and asked for payment of a "delivery fee," clearly a scam.

I also found a real phishing email in my spam folder pretending to be from Microsoft. The the link pointed to a fake login page.

All these cases used urgency and fake domains to trick users.

Always check sender addresses, avoid clicking unknown links, and never share personal or banking information by email.

How quickly do you notice the suspiciousness of a phishing message?
I usually notice it quite quickly because of unusual sender addresses, poor grammar, and urgent or threatening language. The tone and formatting often feel different from legitimate messages.

Would you recognize this message as dangerous without the header?
Yes, most phishing messages can be recognized without checking the header, based on visual clues such as fake links, generic greetings, and unrealistic requests.

What advice would you give to someone who is new to email regarding the dangers of social engineering?
Be careful with any unexpected email. Never click on unknown links or attachments, and never share personal or login information. Always verify the sender's address, and if something seems urgent or "too good to be true," double-check with the official organization before responding.

The analysis of the email header showed that the real sender IP was 185.203.116.10, which originates from Russia. The sender's domain did not match the "From" address the message appeared to come from support@microsoft-verify.com, but the return path pointed to a different domain. The email was also routed through multiple servers, suggesting redirection to hide its true source. In addition, all SPF, DKIM, and DMARC checks failed. These indicators clearly show that the message was a phishing attempt, not a legitimate communication from Microsoft.