Dear x

As many of you have probably noticed, a phishing email was sent out to all employees in the organization on the (insert date of campaign). This phishing email has been developed in collaboration with the Danish IT security company CyberPilot, which specializes in simulated phishing attacks and awareness training. Therefore, no damage has been done. If you’re in doubt, it was the following mail:

(Insert screen dump of email)

The purpose of the simulated phishing attack is to evaluate our responsiveness in such situations and identify where we can do better. The purpose is not to punish anyone, but to make you aware of how you can detect phishing emails and how to deal with this in the event of a real phishing attack.

Overall (you did well / we have something to work on / status of the campaign) You can see the result of the phishing campaign below:

• xx received the phishing email

• xx clicked on the link in the phishing email

•xx unique users submitted data

•xx made us aware of the phishing attempt

(*Here you can write your comment on the results*).

The indicators of phishing you could find in the email are: (examples)

List of elements in the mail that could help identify phishing e.g.

• We would never ask you to sign in just to confirm you have read something.

• The sending email address @xxx - any mail from us would come from an e-mail ending in @xxx

• You are asked to log in with your xxx login on a basic, shady website.

Just to make sure no one is worried about the data that were submitted, the ‘phishing’ page has not saved any of the data, it simply just returned an error page regardless of what was put in the boxes.

I would like to commend all of you who have been aware and reported the email to (the IT department / DPO / etc.) - great work! Remember that you should always contact (IT department / DPO / etc.) if you have the slightest doubt. That way we stand strongest 😊

If you have any questions about the above, please reply to this email or come by our office for a chat.