Dear xxx

As many of you have probably noticed, a phishing/spam email was sent to all employees in the organization on DATE. This phishing email was developed in collaboration with the Danish IT security company CyberPilot, which specializes in simulated phishing attacks. Therefore, no damage has been done. If you’re not sure what I’m talking about, it was the following email:

Insert screenshotof email

The purpose of the simulated phishing attack is to evaluate our responsiveness in such situations and identify where we can improve. The purpose is not to punish anyone, but to train how to detect phishing emails and how to deal with it 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:

* xxx received the phishing email
* xxx clicked on the link in the phishing email
* xxx submitted data

(Here you can write your own comments on the results).

**How can we recognize a phishing email and what is the right thing to do?**

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

* Clue 1
* Clue 2
* Clue 3

List of examples you could list

* We would never ask you to sign in just to confirm you have read something.
* This type of information/call for action would never come without prior information
* The sending email address was @xxx - any email from us would come from an email ending in @xxx
* You were asked to log in with your xxx login on a basic and shady website.

**What is the right thing to do?**

This is described in our IT security policy: Where can it be found/read?

* Procedure: Reminder of your procedure (should be consistent with the IT security policy)
  + If you are suspicious and/or would like to warn that there is a phishing email in circulation
  + If you have interacted with the email (clicked on the link/submitted data/accepted download)
* Person in charge: Name the person responsible for IT (daytime/on-call phone)

I would like to commend the employees who have been aware and followed our procedure/reported the email to (IT department/DPO/etc.) - good job! Remember that you should always contact (the IT department/DPO/etc.) if you have the slightest doubt. In this way, we help each other and stand stronger.

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