Hello everyone,

As part of our ongoing IT security training, we have decided to conduct simulated phishing attacks in collaboration with CyberPilot, a Danish IT security company, who we also collaborate with for our awareness training.

**What is a simulated phishing attack?**

Simulated phishing attacks involve sending emails that mimic typical spam/phishing emails, including potentially malicious links and requests for sensitive information.

Through these simulations, we will be able to track the following:

* Number of email recipients and openers
* Number of people who click a link
* Number of people who submit data

**Why?**
The goal of these simulations is to evaluate our organization's ability to identify and respond to phishing emails, as well as to provide valuable training on how to handle such threats/attacks. This will enable our IT department to identify areas for improvement and enhance our overall security.

It is important to highlight that the purpose of these simulations is not to single out any one, but rather to educate all employees on recognizing and dealing with phishing attacks effectively.

**When?**

We will be conducting one or more phishing simulations in the near future, and we encourage you to view this as an educational opportunity to enhance your awareness of different types of phishing attacks.

We hope that you will see it as a fun exercise that can give you some insight into what different phishing attacks can look like and how you can detect them.

Should you have any questions, please do not hesitate to reach out to xxx.

We look forward to working together to strengthen our security measures and protecting our organization from potential cyber threats.