Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

COMMUNICATION DRAFTS FOR SECUREPOINT AWARENESS PLUS BUILDING

DESCRIPTION

This document contains communication drafts that you can use for your internal communication of the Securepoint cyber security Awareness PLUS building. The free use of this document is included in our service. Please feel free to adjust the drafts for your organizational purposes and customize them to fit your standards and procedures.

We recommend that you pre-announce the phishing simulation to all employees. According to our project experience to date, this has had the following predominantly positive effects:

Chances:

- All stakeholders informed in time - no surprises
- Increased awareness even before the start of the phishing simulation
- Emphasis on the added value of the phishing simulation
- Perception of cyber security awareness as *useful* instead of *annoying*

Risks:

- No pure blind test: slightly lower initial value of the click rate

We recommend using the communication drafts for your data protection officer(s), your IT support, and to give advance notice to your employees before starting the measure. You can use the intermediate communication to share the results with your employees:

First, use communication 1 to share the results with your employees after the first two weeks ("initial phase"). Proceed with communication 2 to keep your employees informed about the current status of the simulation and to give the topics high visibility within your company. (This is optional; however, we recommend that you set up a communication plan to accompany the awareness measure throughout its entire duration.)

This document supports you in conducting this communication without much effort on your part. You can send the final evaluation at the end of each simulation year to communicate the final results and announce its continuation.

Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

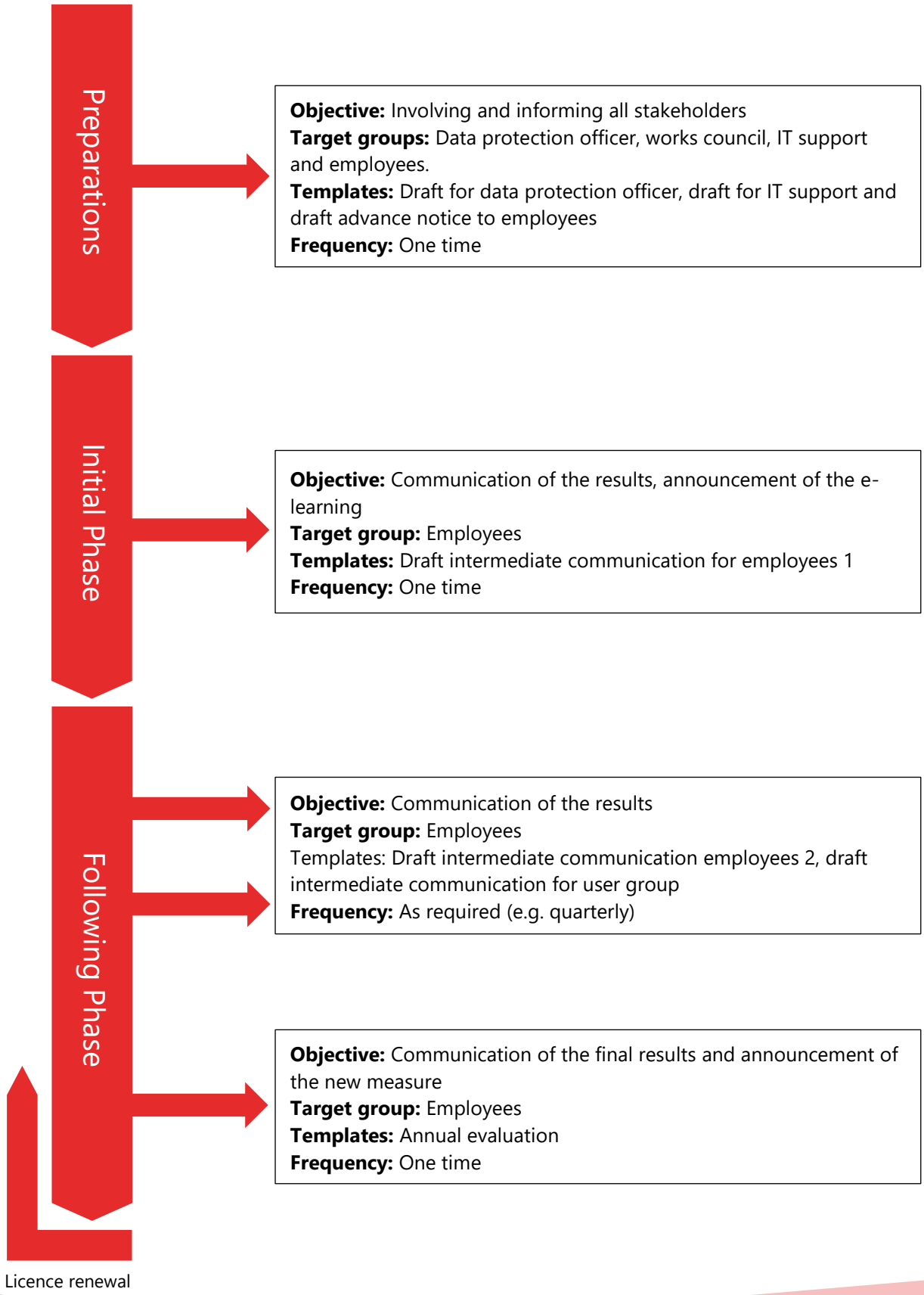
TABLE OF CONTENTS

Please note:

Below you may find parts highlighted in yellow which implies that those phrases must be adapted to your specific circumstances. Additional ***< bracketed components >*** insinuate that the following text passage might not always fit for each customer and awareness package and should be removed from the communication.

Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

OVERVIEW PROJECT PROGRESS AND POINTS OF COMMUNICATION



Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

DRAFT FOR DATA PROTECTION OFFICER

Subject: Information about the Awareness PLUS-Training and request for approval

Dear Mr./Ms. ...,

For your information, I am sending you an overview of a training measure to increase our cyber security awareness. The objective is:

- Evaluating the current vulnerability to phishing attacks
- Training of our employees through simulated phishing attacks
- Minimizing the risk of cyber-attacks for our company

The core element of the training is a 12-month simulation of phishing attacks via prepared e-mails. In total, each employee will receive up to 12 such e-mails during this period. These e-mails are not dangerous, and the links included in them only lead our employees to interactive learning pages. There is no security risk for our employees' equipment or data at any point in time.

The execution of the simulation as well as the processing of the e-mail addresses and personal data (name etc.) of our employees is carried out by our service provider Securepoint GmbH in accordance with the enclosed data processing agreement.

Please understand the phishing simulation as a training offer for our employees - we are not interested in exposing individual employees. The simulation is anonymous. No conclusions can be drawn about individual employees. Only aggregated figures across all employees are recorded, e.g.:

- Opening rate of the respective phishing e-mails
- Click rate on phishing links within these e-mails
- Click rates over time

If you have any further questions, please contact me.

Kind regards

Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

DRAFT FOR IT SUPPORT

Subject: Information about the upcoming Cyber Security Awareness PLUS-Training

Dear Mr./Ms. ...,

This is an overview of an upcoming training measure to increase our cyber security awareness. Our objective is:

- Gain insight into current vulnerability to phishing attacks
- Training of our employees through simulated phishing attacks
- Minimizing the risk of cyber-attacks for our business

The core element of the training is a 12-month simulation of phishing attacks via prepared phishing e-mails. In total, each employee will receive up to 12 such e-mails during this period. These e-mails are not dangerous, and the included links only lead our employees to interactive learning sites. There is no security risk for our employees' equipment or data at any point in time. I am already in agreement with our data protection officer regarding the corresponding DPA with the service provider Securepoint GmbH.

The sender addresses and subject lines of e-mails to our employees can be found in the attached overview. Many of our employees will hopefully recognize these e-mails as phishing attempts and report them to you. I recommend setting up a separate routing for these support tickets in advance. It would be great if you provided me with the number of reported e-mails (related to the above-mentioned phishing e-mails) in a short monthly reporting.

Please keep this list of phishing e-mail templates confidential. In order to maximize the training effect, our colleagues will not receive any details about the upcoming e-mails.

To make the this technically possible, I kindly ask you to include the following mail server sender addresses of our service provider Securepoint in our whitelisting:

- <Please insert the IP address from the Securepoint Manager portal under 'Whitelisting'>

Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Further technical information about Awareness PLUS can be found at https://wiki.securepoint.de/AwarenessPLUS. Please give me a short feedback as soon as this has been done and please do not hesitate to contact me if you have any further questions.

Yours sincerely

Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

DRAFT FOR ADVANCE NOTICE TO EMPLOYEES

Subject: Information about upcoming cyber security Awareness PLUS-training

Dear colleagues,

We have probably all heard about cyber-attacks in the news. Cyber-attacks in both private and professional contexts are constantly on the rise. In order to increase our defence capability against such attacks, we will soon be conducting a cyber security awareness training. Our objectives are:

- Gain insight into current vulnerability to phishing attacks
- Training of our employees through simulated phishing attacks
- Minimizing the risk of cyber-attacks for our business

The core element of the training is a 12-month simulation of phishing attacks via prepared e-mails. In total, each of you will receive up to 12 such e-mails during this period — an average of about one e-mail per month. These e-mails are not dangerous, and the contained links only lead you to interactive learning pages. Nevertheless, we advise you to be cautious, as real attacks using phishing e-mails can happen at any time. Please take this risk very seriously and do not click on suspicious or unknown links or attachments. If you suspect an e-mail to be a (simulated) phishing attempt, forward it to our IT support.

In case you do not recognize the simulated phishing attempt and click on it, you will be redirected to a learning page. Please take the time to read through the information texts to learn how you can recognize phishing e-mails. This significantly reduces the risk of a cyber-attack on our company. You can see an example of the learning pages in the picture below.

Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

There is no security risk for our equipment or data at any point in time. Of course, the simulation is completely anonymous. Neither we nor the service provider Securepoint (https://www.securepoint.de), who performs this simulation for us, can at any time see how you personally click or behave. Securepoint only provides us with an aggregated summary overview of click behaviour.

<When e-learning is part of the awareness measure>

In addition to the phishing simulation, you will soon have access to a special e learning offering. Easily digestible e-learning modules will be available, each with an exciting quiz. The acquired knowledge is also very valuable for your private context at home!

Please help make us all safer against cyber-attacks! If you have any questions, please do not hesitate to contact me.

Yours sincerely

Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

DRAFT FOR INTERMEDIATE COMMUNICATION TO EMPLOYEES 1

Subject: Information on the ongoing cyber security Awareness PLUS-training

Dear colleagues,

as many of you have surely noticed, we have carried out a somewhat different kind of sensitization on the topic of cyber security and the secure handling of e-mails in recent weeks.

Phishing Simulation

As part of a phishing simulation with the security company Securepoint GmbH, you have all received some e-mails that were based on realistic phishing attacks on our company. Additional information on such a simulation can be found in a compilation of the most frequently asked questions at https://wiki.securepoint.de/AwarenessPLUS. Those of you who have clicked on the phishing links in these e-mails were able to find out about how to recognize and deal with phishing e-mails.

For those who have not responded to any of the phishing e-mails, we have listed the links to the corresponding learning pages with all the hints here:

- ...

In total we have reached a click rate of XX% on the phishing links.
<When e-learning is part of the awareness measure>

E-learning

While the phishing simulation will continue in the upcoming months (with reduced intensity), you will be able to deepen your knowledge about cyber security and phishing. From **xx.xx.xxxx** onwards we offer you access to special e-learning modules on cyber security. These modules are very compact and include an exciting quiz at the end. You can determine your personal level of knowledge through your SafeScore.

With the start of the e-learning you will receive an invitation e-mail from Securepoint -GmbH (noreply@awareness.securepoint.de) to register.

We hope to offer you a varied learning experience. These e-learnings are very practical and designed to use the knowledge in your private context as well. They contain short videos — so feel free to use your speakers, if available. However, you can also complete the modules without sound. If you have any problems with the Securepoint learning platform, please visit https://wiki.securepoint.de/AwarenessPLUS.

Kind regards

Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

DRAFT FOR INTERMEDIATE COMMUNICATION TO EMPLOYEES 2

Subject: Feedback on the ongoing Cyber Security Awareness Training

Dear colleagues,

As all of you are aware, we have been running a phishing simulation with the security company Securepoint GmbH for some time. The simulation has been active in our company for X months and each of you will have had contact with the sent e-mails in one way or another.

We wanted to reach out to you again to inform you about the current status of the simulation.

The click rate is currently at XX%, which is an improvement/deterioration of X% compared to the last communication.

<In case of an improvement>

We would therefore like to take this opportunity to expressly commend you for handling your e-mails so responsibly and attentively. By doing so, you are actively contributing to the security of our company.

Please continue to remain alert and check all e-mails that seem suspicious to you, regardless of whether they originate from the simulation or not. IT security concerns us all!

<In case of a deterioration>

Unfortunately, the results have deteriorated during the current simulation. Please keep in mind that the damages caused by a successful phishing attack usually costs millions. Therefore, we ask you to treat this simulation with the same seriousness as real phishing attacks. We count on your help also to prevent a worst-case scenario.

< When e-learning is part of the awareness measure >

Also, we would like to encourage everybody to make use of the Securepoint Awareness PLUS e-learning platform. It will help you to prepare for different scenarios of cyber-attacks in the best possible way and help you determine how to handle them. If you are not yet registered, please do so today at https://awareness.securepoint.cloud/register.

IT security concerns all of us!

Many greetings

Securepoint GmbH
Bleckeder Landstraße 28, D-21337 Lüneburg
Tel.: +49 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

DRAFT FOR COMMUNICATING THE ANNUAL EVALUATION

Subject: Final evaluation of the current awareness measure

Dear colleagues,

At the end of the current cyber security awareness measure, we would like to get back to you with a short evaluation regarding the results of the phishing simulation.

At the beginning of the phishing simulation, we achieved a click rate of XX%, after a year of continuous training, our click rate is currently X%. This corresponds to an overall reduction of X% and amounts to a total of X clicks. We would like to congratulate you all on this accomplishment.

We have also achieved a very important reduction in the interaction rate, which for example records the activation of macros or the entry of login data. At the beginning of the simulation, we had an interaction rate of XX%, currently it is at X%.

We would like to congratulate you on the improvements achieved. At the same time we would like to take this opportunity to point out that there is still room for improvement in the following areas:

- • ....
- • .....
- • .....

For those who have not clicked on any or only a few of the phishing e-mails, we would like to provide you with a list of the links to the corresponding learning pages. Please take the time to familiarize yourself once more with the different tactics used in phishing mails:

- • ...

To keep our cyber security at a high level and to continuously raise the security awareness of all employees even more, we will soon continue the simulation with new mails and e-learning modules.

Kind regards