SECURA PHISHING SERVICES

Increase awareness by assessing and educating

PROTECT AGAINST THE NUMBER ONE THREAT BY ASSESSING AND EDUCATING YOUR EMPLOYEES

One of the most successful methods to attack organisations and individuals is phishing. Using e-mails, WhatsApp, Instagram or other social media, people are tricked into clicking on malicious links, entering passwords or downloading and opening attachments. Attackers attempt to acquire login credentials, credit cards, banking details or personal information in order to take control of the accounts and systems of the people that are being phished.

Phishers are getting better and better, and it is critical for organisations to evolve their security posture with this in mind. The phishing mails full of spelling and grammar mistakes are mostly a thing of the past. These days the phishing e-mails are virtually indistinguishable from legitimate e-mails .

Security-aware and mature organisations strive to protect their business and employees against phishing attacks by training and assessing resilience. By exposing employees to controlled (simulated) phishing attacks, they will learn to better recognize the methods attackers use and differentiate a phishing attempt from harmless (legitimate) messages. Exposure to (and showing the consequences of clicking on) malicious links, is a very effective training method.

SECURA'S PHISHING SERVICES

Secura has developed an easy and standardised way of creating phishing campaigns for training and awareness purposes. Our Angler platform lets you choose from a number of templates for the phishing mail, all with their own scenario and landing page. Each scenario leads to a landing page, where a message is displayed that informs the user that this was, in fact, a phishing attempt. The page further provides guidance on how to recognize such e-mails in the future. Optionally, users can be asked to enter their credentials before this message is shown, in order to measure their willingness to disclose their passwords. This metric is especially good to measure the progress of awareness campaigns over time.

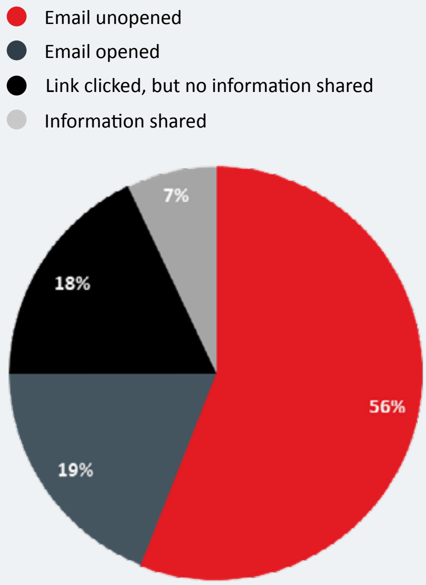
Based on our extensive experience, we have developed a number of successful scenarios. For instance:

- A catering survey
- An office survey
- “Reward your colleague”
- Order your new key card
- “Verify your account details”
- Salary approval

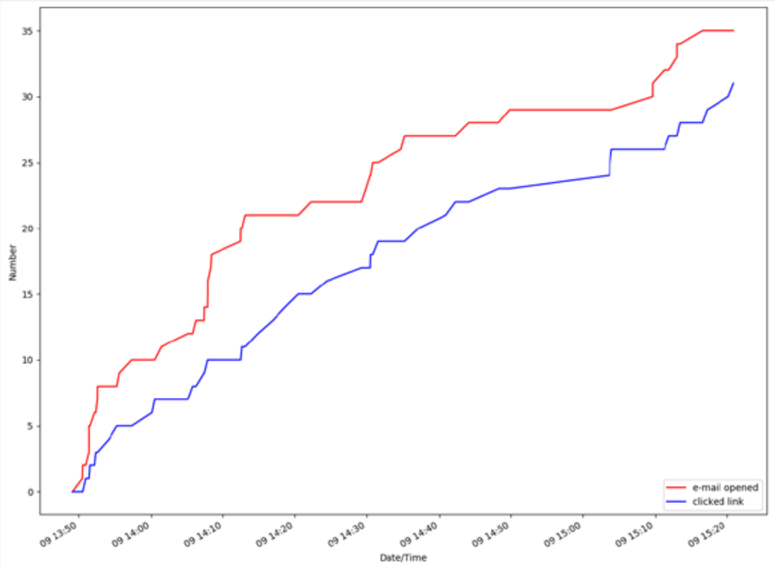
Secura provides clear and concise reports, where customers can filter and report based on aspects such as organisation, department or function group. This enables you to track progress over multiple campaigns and direct attention where it is necessary.

In addition to our simulated phishing service, Secura can also provide awareness campaigns for all layers of the organisation. Combined, this provides a measurable way to improve the security posture of all employees, thereby improving security behavior and lowering the risk of exposure to malware, credential theft, or worse.

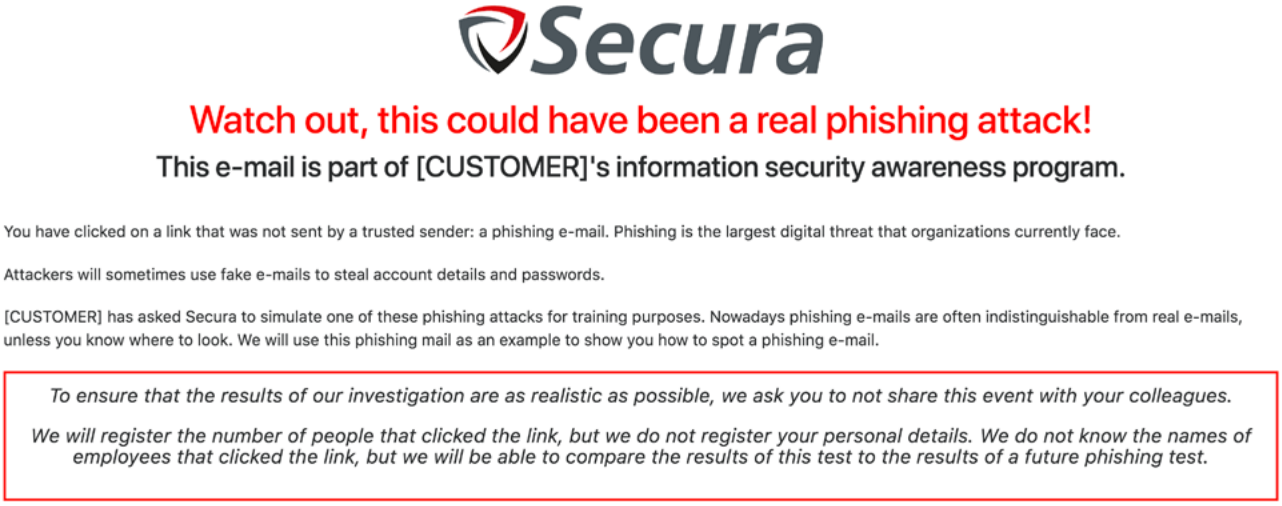
SAMPLE RESULTS



Number of emails opened and links clicked in the first 90 minutes after receiving Secura's phishing email.



SAMPLE OF SECURA'S PHISHING EMAIL LANDING PAGE



Watch out, this could have been a real phishing attack!

This e-mail is part of [CUSTOMER]'s information security awareness program.

You have clicked on a link that was not sent by a trusted sender: a phishing e-mail. Phishing is the largest digital threat that organizations currently face.

Attackers will sometimes use fake e-mails to steal account details and passwords.

[CUSTOMER] has asked Secura to simulate one of these phishing attacks for training purposes. Nowadays phishing e-mails are often indistinguishable from real e-mails, unless you know where to look. We will use this phishing mail as an example to show you how to spot a phishing e-mail.

To ensure that the results of our investigation are as realistic as possible, we ask you to not share this event with your colleagues.

We will register the number of people that clicked the link, but we do not register your personal details. We do not know the names of employees that clicked the link, but we will be able to compare the results of this test to the results of a future phishing test.

INTERESTED?

Would you like to learn more about our services?
Please do not hesitate to contact us.

Follow us on

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com