Deloitte.

Phishing as a Service

June 2018

Risk Advisory

Contents

Stop phishing attacks

Tell me and I forget, teach me and I may remember, involve me and I learn.

As computer systems become increasingly complex, the human component becomes an interesting entry point for attackers. Research shows that in 29% of successful data leaks, employees provided access to attacker unintentionally.

Phishing is the practice where cyber criminals email employees asking them to perform a certain action e.g., clicking on a malicious link which installs software and allows an attacker to gain access to sensitive data or take control over the system.

To educate employees about phishing, organizations often offer trainings and conduct awareness campaigns. However, the knowledge fades with time which makes it imperative to have these training and awareness campaigns to be repeated periodically.

We suggest a continuous phishing awareness campaign, where employees are trained and assessed with periodic simulated attacks. These campaigns would help in educating the employees on real time scenarios and complement existing security workshops.

Understanding the threat

To protect an organization against phishing, it is necessary that employees understand how cybercriminals work. A common attack vector is to spoof the email address of the sender, e.g., pretending to be a trusted colleague. Employees tend to fall for this trick as it is common human behaviour to help others in need, which the attackers take advantage of.

How to respond

To quantify the risk of phishing within your organizations, it is necessary to measure employee behavior in a privacy preserving and ethical manner. We provide the means to measure employee behaviour through customized stimulated phishing attacks as part of the ongoing learning cycle. The awareness is reinforced by a follow-up e-learning module on phishing.

The number of technical security measures within organizations is increasing over the past years. As a result, attackers are focusing more on the weakest link: the human factor. Phishing is a method whereby malicious e-mails are sent by cybercriminals with the intent to gai rst point of entry into the corporate network. Educating employees to recognize and respond to phishing attacks is the best step towards a more secure organization.

A combined solution

Our comprehensive approach starts with an awareness campaign and is followed up with the following actions:

Campaign Preparation

1. Phishing test - Testing the susceptibility of your employees
2. Improving the phishing awareness
3. Monitoring the awareness improvement

The awareness campaign begins with introducing the employee to the subject of phishing. During this introduction, the employee will gain knowledge about phishing, and the employee will be informed that at a given moment, they will get first-hand experience with a phishing attack and an e-learning.

1. Phishing Campaign

Before the test begins, Deloitte works with the organization with the necessary preparation, such as how to deal with higher volume on the IT-services, inform help desk to handle potential employee reactions and help in deciding the right phishing scenario.

When testing starts, Deloitte sends the crafted phishing e-mails to the (targeted) employees and measures a few parameters, such as how many employees click the malicious link, at what time were the links opened, what type of information the employees disclosed, and the success rates among departments or business units. If the test is part of a recurring service, Deloitte can also provide trends between tests, so the organization can determine the e ctiveness of its awareness campaigns.

The infrastructure for executing the phishing tests is internal and assures the privacy of the shared information and the link between the employee and the results is preserved.


Deloitte.

Sinterklaasactie

Wat staat er op jouw verlanglijstje?

Beste collega,

Deloitte.

Tomorrow is Today

Tomorrowland VIP packages

Dear colleague,

2. E-learning

After the test, the employees can be informed about the results and what can be learned from these actions. As part of this feedback, Deloitte has also developed an e-learning module including th nal online exam. E-learning provides insight into the threats, educates the employees how to (re)act during an actual attack, and improves the overall security awareness of the employee. Because the e-learning closely follows up on the phishing test, the employees are usually very interested in the material.

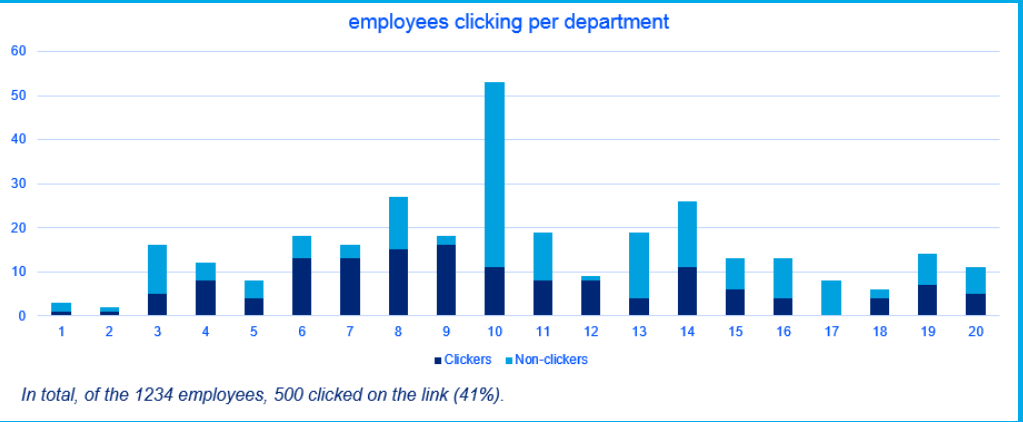
The e-learning can be customized for the organization, which ensures better transfer of knowledge.

The e-learning does not solely focus on the technical aspects, but also covers other areas such as psychology and business impact. With a preliminary questionnaire, the content of the e-learning is dynamically adjusted to the level of knowledge of the employee. The e-learning can be provided in parallel with a workshop about general cyber security awareness to raise the overall awareness and answer related questions.

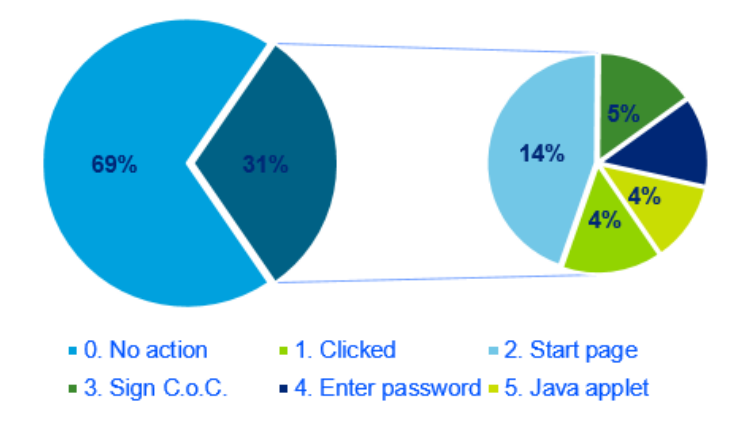
3. Monitoring Improvements

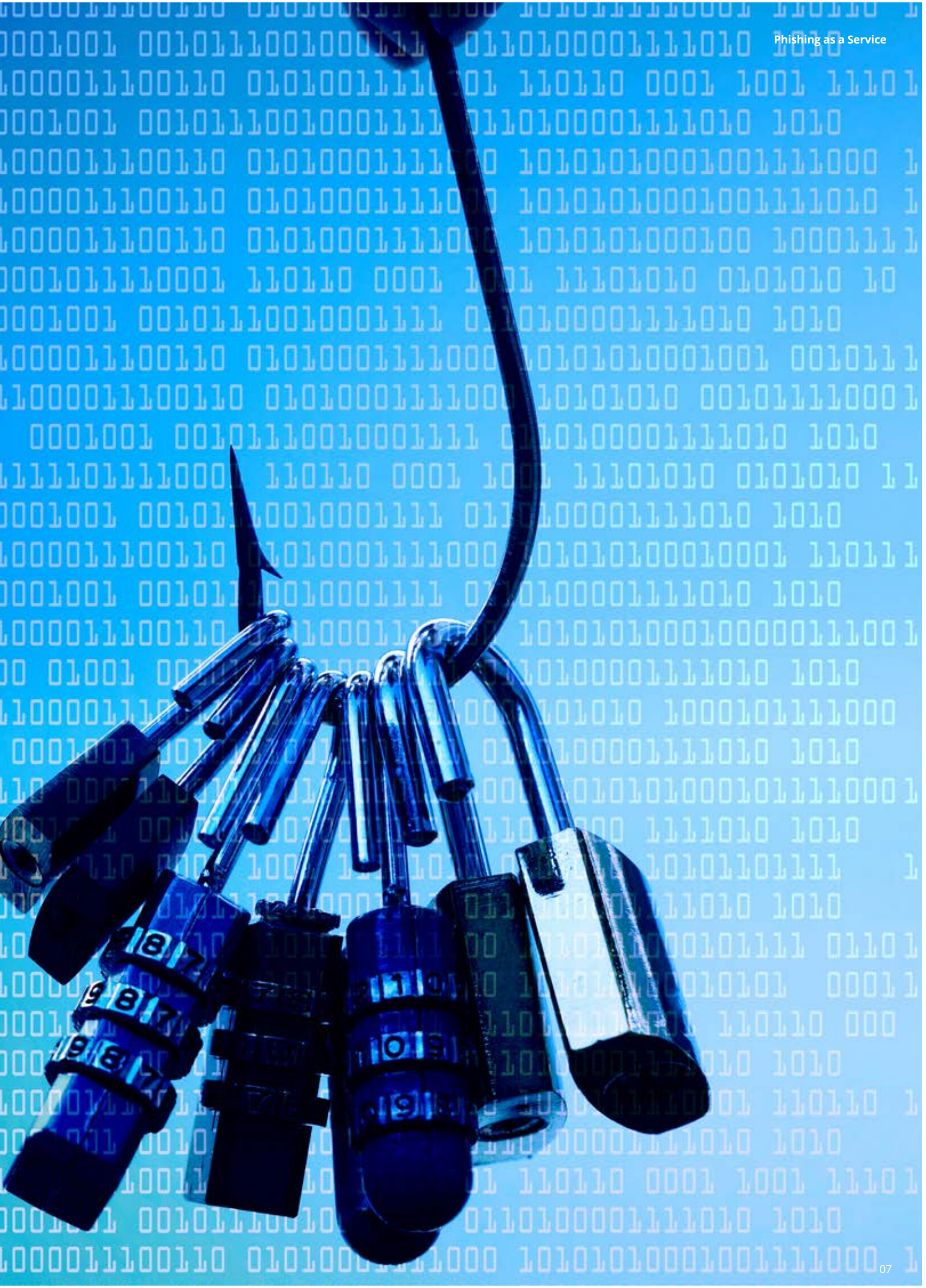
The final step in the process is making the test results measurable and presenting them after they have been anonymized. We regularly track the results and monitor the awareness level. In addition, the result can be used as input for consecutive phishing tests.

Deloitte offers a dashboard with statistics of the awareness level in regard to phishing within your organization. The statistics will not only offer insight into the progress within your own organization but also allow you to see how your organization is doing in comparison to peers.



In total, of the 1234 employees, 500 clicked on the link (41%).





Why Deloitte

Deloitte has a broad range of experience when it comes to consultancy and assessment of information security within both private businesses and government institutions.

- Deloitte has plenty of experience with securely performing phishing attacks and reliably training organizations.
- Deloitte has an infrastructure to send thousands of e-mails per minute and store results securely and anonymously.
- Deloitte used the infrastructure, the training materials, and the e-learning course for a number of clients. They are e ective and can be easily tailored to provide a custom training, speci c to the organization.

Deloitte leverages its Cyber Intelligence Centre (CIC) to deliver “Phishing as a Service” to its clients across the globe. The CIC combines deep cyber intelligence with broad business intelligence to deliver relevant, tailored, and actionable insights to inform business decision-making.

The CIC fuses a number of services together to provide our clients with a truly tailored service that enables them to fully understand their cyber risks and adopt proportionate responses in an increasingly digital and interconnected business environment. We do this by providing them with improved visibility of threats and assets, based on highly relevant intelligence that re ects their speci c business, market, and industry context.

Key Contacts:

Rohit Mahajan
President - Risk Advisory
rmahajan@deloitte.com

Gaurav Shukla
Partner - Risk Advisory
shuklagaurav@deloitte.com

Anand Tiwari
Partner - Risk Advisory
anandtiwari@deloitte.com

Sandeep Kumar
Partner - Risk Advisory
kumarsandeep@deloitte.com

Deloitte.