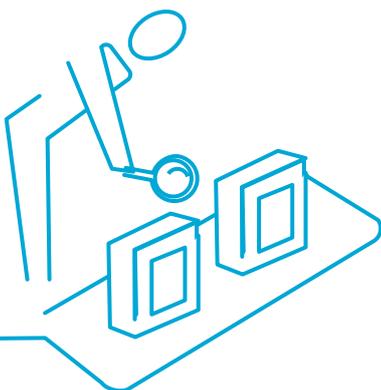


Are your employees aware of phishing risks?



Find out with the Capgemini Phishing audit

With the ever increasing use of new channels and technology, the risk of cyber attacks is increasing accordingly. Cyber crime, corporate espionage and hackers pose serious threats and call for appropriate measures that go beyond the IT domain. These threats affect the continuity of business, corporate reputation, liability for customer and personal data, and the according costs of it. Your systems may be well secured, but what about the way of working of your staff? Without knowing, an inattentive employee could easily open the digital doors for hackers to confidential information of your company or worse... of your clients. One of the frequently used methods that hackers use to find a way into your corporate network is phishing. As part of our Cybersecurity awareness campaign, Capgemini has developed a Phishing Audit, shaking up your staff with a fake, yet realistic phishing attempt, and find out how many of your employees take the bite. With the phishing audit you measure and raise the awareness level in your organization before a serious phishing attempt is made.



What is phishing?

Phishing is the term for activities aimed at obtaining personal data from people by sending legitimate-looking emails. Obtained personal information can be used for e.g. corporate espionage, to obtain intellectual property and credit card fraud. It appears that more than 80% of cyber attacks start with a phishing email!

It is already happening

Literally everyone is targeted with phishing. A common practice is to get user credentials of one of the administrators to gain access to the systems to exploit. Since then they capture large amounts of confidential data and sabotage corporate computers. A recent example of a successful phishing attack is the hack on a major US bank, where criminals conducted a large-scale phishing attack and stole millions of personal account information. And the number of cyberattacks is increasing rapidly.

Testing resilience and vulnerability

A phishing audit is a security audit based on the principles of phishing. It is a method to test the resilience and vulnerability of employees against phishing by simulating a phishing attack and measuring the response to the phishing emails. At the same time a phishing audit directly increases security awareness among employees.

How does it work?

Of course our phishing audit is well controlled and in line with privacy regulations, though the impact on your staff will be the same as with a real attack. Which is exactly what we want to achieve. In phase one we establish the goals and scope of the audit, after which we develop customized phishing scenario's with a representative of your company. In phase two we build phishing emails, websites and set up the environment. Our simulated attack can be executed in just one day, and after the attack we inform your staff about the audit and gradually raise the awareness levels in your company. Finally we analyze how people reacted. We collect results and report outcomes and practical improvements. Optionally we measure the improvements in detail and provide hands on support for more cybersecurity awareness. The entire audit process is carried out in approximately two weeks.

Homemade, home tested

To make sure the audit does contribute to awareness in the organizations of our clients, we regularly carry out a phishing audit within our own company. Our employees are aware of the threats. If you want the same for your staff and make sure they don't take the bite, let us carry out a phishing audit in your organization. The next attack may well be not as friendly as ours.

For more details contact:

Capgemini Nederland B.V.

Matthijs Ros

Leader Cybersecurity
matthijs.ros@capgemini.com
Tel. + 31 6 4570 6660

Guido Voorendt

Cybersecurity Consultant
guido.voorendt@capgemini.com
Tel. +31 6 2954 1836



About Capgemini

Now with 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2014 global revenues of EUR 10.573 billion.

Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at
www.nl.capgemini.com