sepago®

PHISHING AWARENESS

sepago. making people love it.

In **2020**, the way we work has **changed fundamentally**. A lot of organizations moved to **working from home** at least partially. For IT departments, this meant completely new requirements in **building a secure modern workplace** to enable business continuity.
One of the focus are, of course, **cyber attackers**. Recently, cybercrime has become a business. Almost self-explanatory, attackers have taken advantage of the **home office situation** and increased digitalization. This **illegal business** is acting professionally, and a constant **cat and mouse game** has emerged. Companies try to make their environment secure, and hackers try to break them.

Attack Simulation Training

Agenda

1. **Awareness**
   Communication plan & material
2. **Kick-off-Workshop**
   Tool demo
   Process assessment
   End-user Reward model
3. **Monitoring & metrics set-up**
   Measurement plan/ Scorecard
   Dashboard implementation
   API connection
4. **Development & documentation operational model/ process**
5. **Development & documentation Implementation plan**
6. **Close out & defined next steps**

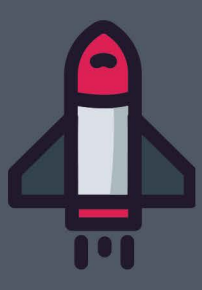
We at sepago want to support organizations in solving the described dilemma!

Starting not from pure technology, but from use cases, we create a target picture for you based on best practices from the Microsoft universe and completed customer projects.
We will offer you an Attack Simulation Training as realistic as possible. It is our goal to achieve that your employees recognize external attacks and does not falling for professional Phishing and Malware campaigns.
Because user attention is the holy grail, it is very important that current and realistic campaigns are used. In addition, the attention of the employees is achieved in the best way possible, when they learn from realistic content and scenarios.

In most companies you have **four groups** of people who faces serious issues into the context of **phishing simulation**.
First, **Security Operation** has a lack of guidance and time when it comes to selecting simulations to run on their company.
The next group is the one of the **end users**. The Training is generic and disconnected from reality and therefore less effective.
The third group of **CISO's** are unsure how or what to measure to determine if training is having any impact.
And the last group of people within the organization who faces serious issues in the context of phishing simulation is the **IT Controlling**.
Because extra phishing simulation cost extra licenses.

Now, to find an all-encompassing solution sepago offers you an Attack Simulation Training. We will find the best solutions for you to achieve your targets in Phishing Awareness.

Phishing Awareness with sepago will help you to protect your company against attackers in an easy, realistic and up-to-date way.
With sepago, your company can increase the resistance to IT attacks and reduce attacks and alarms in the system by up to 45%!



PLEASE CONTACT US
ANJA KRUMKAMP
IT Security Sales

+49 221- 801 93 95 0
anja.krumkamp@sepago.de

sepago GmbH
Dillenburger Straße 83
51105 Köln

Tel.: +49 221-801 93 95 0
info@sepago.de
www.sepago.de

Partner
Microsoft
citrix.

Always informed with sepago: