Add value.
Inspire trust.

Simulated Phishing Attacks Services

Simulate a phishing attack and train your employees to protect against cyber threats

Your challenges

The last few years have seen some massive changes in the way we work - from migration to a hybrid workplace to rapid digital transformations, to an increase in the use of AI technologies. As organisations continue to embrace these new ways of working, there is an increase in phishing attacks too. But despite the real threat that phishing poses to businesses today, almost 1 in 5 organisations just deliver phishing awareness training to their employees once a year. This lack of awareness is a large contributing factor to the fact that social engineering—attacks that manipulate the user into giving information to a cybercriminal—remains the threat type most likely to cause a data breach. In fact, according to Verizon's 2022 DBIR, 82% of data breaches involve a human element, including phishing and the use of stolen credentials.

What is Simulated Phishing Attacks Service?

Simulated phishing attacks offer a proven high value addition for all organisations where people work with digital systems. Almost 90% of current cyber-attacks can be traced back to human error - this has been shown by various studies.

Why is it important for your organisation?

Phishing emails are often used as a gateway for malware or blackmail attempts (ransomware). Without targeted training, it is easy for attackers to deceive the e-mail recipient (the employee), and prompt them to do activities that can threaten the security of the company. It is therefore extremely important to train employees regularly. Regular training courses improve the resilience of employees against phishing attacks.

At TÜV SÜD, we simulate a phishing attack on your organisation or on specific areas of your company and prepare your employees for cyber threats. There are various phishing scenarios to choose from, such as: clicking on links, opening attachments, accessing information via a data mask. We can customise the content of the scenarios for your company and the desired target group. In addition to an anonymised report with click rates and information on disclosed data, you will receive specific recommendations for

corrective actions. As an additional option for simulated phishing attacks, you can choose to have informative online training courses and/or learning materials to be attached to the e-mails. These training courses open automatically after a user clicks on the alleged phishing e-mail. Your employees will be trained immediately.

Our service mainly relates to the international standard ISO 27001. This covers the entire cycle of information security and requires, among other things, that your employees are involved in cyber security measures. With our training, you can meet this requirement and help your company to protect itself from one of the greatest cyber threats.

TÜV SÜD's Simulated Phishing Attack Services are conducted as below:

- Firstly, our phishing experts will clarify the following points with you:
  - Number of employees to be tested (email addresses)
  - Define the test period
  - Clarification of the server settings (whitelisting)
  - Clarification of the design and content of the phishing email
  - Clarification of the subsequent learning content (optional)
- Secondly, we start a test to ensure that the e-mails reach your recipients. If this test is successful, we start the simulation at the desired time
- Thirdly, we produce an anonymised report with the click rates and information on the disclosed data. You will also receive specific recommendations for corrective actions from us

Your business benefits

Customised services - We design the phishing attacks individually and tailor them to your organisation. Also, we can use a database with more than 1,000 different templates for phishing emails. These are updated monthly and are available in different languages

Anonymous evaluation - You will receive an anonymised evaluation including a report

Ensure higher recall - You have the option of attaching online training courses and learning materials directly to the phishing simulation. These learning units can be processed by employees immediately after the simulation. This leads to a higher recall of the training materials

Why choose TÜV SÜD?

TÜV SÜD's experts are specialists in cybersecurity assessment, training, audit, and certification. With our experts' knowledge, they are here to consult and recommend. From cyber risk assessments and cybersecurity training, to carrying out security certification projects, our industry experts have successfully helped companies to improve their cybersecurity. With a structured approach to cybersecurity services developed from many years of experience, domain specific know-how and regulatory expertise, TÜV SÜD offers support to companies across a range of sectors. By helping organisations with compliance to global security standards, TÜV SÜD has ensured our clients have access to markets across the world.

Our Head Offices in South Asia, ASEAN, Middle East and Africa Region

INDIA
Tel: +91 1800 212 2000
Email: info.in@tuvsud.com
www.tuvsud.com/in

SINGAPORE
Tel: +65 6778 7777
Email: info.sg@tuvsud.com
www.tuvsud.com/sg

ABU DHABI
Tel: +971 2 676 7600
Email: info.me@tuvsud.com
www.tuvsud.com/ae

AFRICA
Tel: +27 13 244 1330
Email: info.za@tuvsud.com
www.tuvsud.com/za

Follow us on social media linkedin.com/company/tuvsud

TÜV SÜD South Asia Pvt. Ltd. Solitaire, 4th Floor, ITI Road, Aundh, Pune - 411 007, Maharashtra, India.
1800-212-2000 info.in@tuvsud.com www.tuvsud.com/in