DTS

DTS
Security Awareness Training

Security Awareness Training

The modern IT threat landscape clearly has a number of human elements in addition to technical factors. This "human factor" is a popular target for cyber attacks. The majority of these attacks start with an email. While technologies exist to detect and block dangerous emails, the ultimate security is provided by the end user. They are the final hurdle to overcome, because the security of sensitive company data stands and falls with them. Security awareness training is therefore essential to reduce the likelihood of successful phishing or ransomware attacks through effective threat simulations and advanced training. Our Proofpoint Security Awareness Training (PSAT) is unique in the field, using industry-leading risk intelligence and scientific learning principles to deliver the right training to the right people at the right time. We significantly strengthen your last line of defense.

- Integrated security awareness training
- Individuelle, zielgerichtete, interaktive Schulungs-module mit voller Flexibilität
- Phishing simulations
- Optimization of user behavior & response to phishing attacks
- Reporting
- Unlimited platform usage
- DTS managed services

The PSAT is based on a four-part methodology invented by three researchers and faculty members at Carnegie Mellon University. In their research for the National Science Foundation and the Department of Defense, they realized that traditional training methods are not effective in actually reducing risk and vulnerability to cyber attacks. Instead, they developed continuous training, with short, interactive, game-based training sessions, and the use of simulated phishing attacks. This has been shown to be more effective in changing behavior.

The first step in integrated security awareness training is to identify the risk, who is being attacked and what protection options are available. To this end, ThreatSim and CyberStrength can be used to simulate attacks and develop a basic knowledge. Proofpoint's industry-leading threat intelligence accesses data from billions of B2B and B2C emails. In this way, realistic dynamic threat simulation phishing templates can be created. All in all, what emerges in this way is a baseline measurement of the identity of very attacked people (VAPs) and the attacks they come across. The key priorities can then be set.

In the next step, awareness can be developed specifically through interactive training modules to bring about behavioral changes. Proofpoint's training is unique in this regard. It is designed in response to actual threats and user behavior with learning science principles. Training content is continually updated to reflect evolving best practices and current attack trends identified through threat intelligence. The effective, interactive, video-based and gaming training modules encourage learners to fill knowledge gaps about cybersecurity threats in the workplace and beyond. They also provide instant feedback.

Once your users are trained, they will be able to report potential attacks. This reduces the potential area of attack. Closed-loop email analysis and response (CLEAR) further streamlines end-user reporting and security response to phishing attacks. This reduces the time needed to neutralize an active threat. To this end, the PhishAlarm email reporting button and PhishAlarm Analyzer prioritization engine are connected to threat response auto-pull (TRAP).

PSAT is completed by the reporting tools. They provide all the end-user risk information so you can focus on the areas, issues and best practices that will benefit you the most. Reports track user knowledge levels, overall performance of a phishing campaign and detailed information about user performance in each training module, and allow sorting and filtering of all reports based on user-defined properties. These insights help administrators deliver personalized training to achieve measurable results.

- Customization Center
  - Edit training content, including text/questions
  - Add or remove images or questions
- Add policies, certificates and more through the training jackets
- Module configuration

Right People

Only company that can identify people receiving actual attacks and map the training they need to take.

Right Education

Targeted training improves skills to defend against threats received. Proven learning science approaches ensure longer learning retention.

Right Time

Training delivered is based upon actual threats or responses to assessments to ensure relevancy and timelines.

Die Assessments, simulierten Angriffe und interaktiven Schulungsmodule sind in mehr als 35 Sprachen verfügbar. Hierbei werden die Inhalte nicht einfach nur übersetzt. Sie werden entsprechend den Konventionen lokalisiert. Elemente wie Domänen, Marken oder Logos, Charaktere, Währungen und regionale Bezüge sind sprachlich angemessen und schaffen eine persönliche, relevante und ansprechende Schulungserfahrung für den Endbenutzer.