

# Phishing Awareness

---

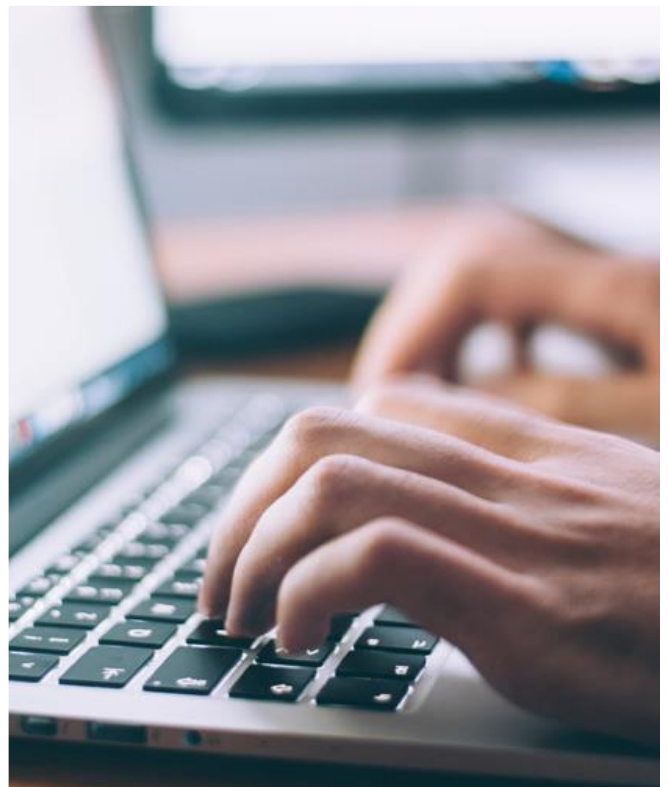
**Training für Mitarbeiter**

**Die beste Abwehr gegen Cyberangriffe sind aufgeklärte Mitarbeiter**



## Warum ist Phishing so gefährlich?

Vor einigen Jahren erkannte man Phishing-Mails schon aus einer Meile Entfernung. Heute erreichen betrügerische E-Mails eine immens hohe Qualität. Hacker recherchieren im Vorhinein Informationen über Kollegen und den Betrieb. Mit Hilfe dieser vertrauten Informationen bewegen sie den Empfänger dazu, seine persönlichen Daten einzugeben oder auf einen schädlichen Link, der zur Installation von Malware führt, zu klicken. Sobald die Schadsoftware auf dem Firmen-Computer installiert ist, kopiert, stiehlt oder vernichtet sie Daten, um danach den Versuch einer Erpressung, die zur Herausgabe oder Wiederherstellung der manipulierten Daten führen soll, zu unternehmen. Jede zweite Firma wurde bereits Opfer eines Phishing-Angriffs. Der Schaden geht in die Milliardenhöhe.



## Wie können sich Unternehmen schützen?

### Security Awareness Trainings

IT-Sicherheit funktioniert nur als ganzheitliches Konzept. Die wichtigste Abwehr ist ein aufgeklärter Mitarbeiter, denn IT-Sicherheit beginnt beim Mitarbeiter. Neben den nötigen technischen Lösungen bieten wir Ihnen daher auch Security Awareness Trainings an. Sie wählen hierbei zwischen einer einmalig simulierten Phishing-Kampagne oder unserem Awareness-Paket mit fortlaufenden Phishing-Kampagnen, Reporting, E-Learnings und Prüfungen.

### Umsetzung der gesetzlichen Vorgaben

Mit unseren Security Awareness Trainings erfüllen Sie eine wichtige Vorgabe der DSGVO. Indem Sie nachweislich Maßnahmen zur Weiterbildung Ihrer Mitarbeiter im Bereich IT-Sicherheit ergreifen, handeln Sie DSGVO-konform und können jederzeit den Lernerfolg Ihrer Mitarbeiter einsehen, grafisch generieren und bei Bedarf vorlegen.



1

## Option: Einmalige Kampagne

Sie möchten die Reaktion Ihrer Mitarbeiter auf Phishing E-Mails testen? Mit unserem einmaligen Phishing Awareness Training sensibilisieren wir Ihre Mitarbeiter für den richtigen Umgang mit E-Mails. Anhand von Klick-Auswertungen realitätsgetreu imitierter Phishing E-Mails erhalten Sie eine fundierte Aussage über den Umgang mit täglich vorkommenden Cyber-Angriffen in Ihrem Unternehmen. Sie wählen dabei zwischen den Phishing-Stufen 1 (Versand an mehrere E-Mail-Verteiler wie z.B. „info@“), Stufe 2 (Versand an Einzelpersonen) und der Zusatzoption Stufe 3 (individuelles E-Mail-Design nach Ihrem Wunsch). Optional folgt eine gezielte E-Learning Schulung inkl. Multiple-Choice-Prüfungen, um Ihr Unternehmen zukünftig stärker vor Cyber-Angriffen zu schützen.



2

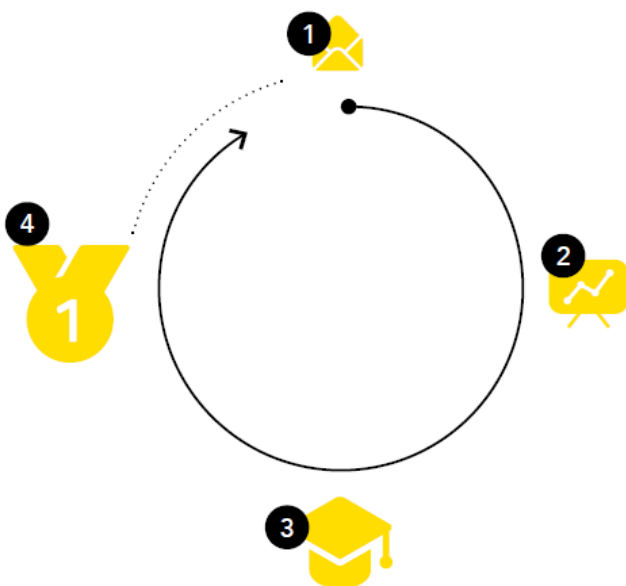
## Option: Awareness-Paket

Erfolg durch Wiederholung! Innerhalb von 12 Monaten führen wir zwei unterschiedliche Phishing-Kampagnen bei Ihnen durch, samt Reporting, Schulungsmodulen und Prüfungen u.a. zur aktuellen Bedrohungslage, Sicherheit am Arbeitsplatz, Social Engineering, Passwortschutz und weiteren interessanten und aktuellen Themen. Das Reporting im Anschluss an die Phishing-Kampagne belegt die Entwicklung der entstehenden Security Awareness in Ihrem Unternehmen. Das Modell basiert auf einer geringen monatlichen Pauschale und ist monatlich kündbar. Ein individuelles E-Mail-Design (Stufe 3) ist hier nicht automatisch enthalten, kann aber selbstverständlich zusätzlich umgesetzt werden.

## Inhalt Awareness Paket

Mit unserem Awareness-Paket halten wir durch fortlaufende Maßnahmen das Thema Awareness in den Köpfen der Mitarbeiter präsent und bauen eine nachhaltige Lernkurve auf. Unser Awareness Paket beinhaltet zwei Managed Phishing Kampagnen innerhalb von 12 Monaten inklusive Vorlagen für eine interne Ankündigungs- und Aufklärungsmail, Durchführung einer Phishing-Simulation und Messpunkten durch das grafisch aufbereitete Reporting.

Außerdem haben die Mitarbeiter **Zugang zu unserer eLearning-Plattform** (Häufigkeit nach Absprache) mit leicht verständlichen Schulungsmodulen zu relevanten Themen. Nach einem kurzen Abschlussquiz erhalten sie ein Teilnahmezertifikat (Nachweispflicht DSGVO, ISO-Standards, Cyber-Versicherer, ISMS). Weiterhin können sie dauerhaft kostenlos unser Browser-Plugin NBDetector zur Warnung vor gefährlichen und gefälschten Internetseiten nutzen.



**1\_Bestandsaufnahme:** Die erste Managed Phishing Kampagne zeigt anonymisiert das Klickverhalten der Belegschaft zu Beginn der Awareness-Förderung auf.

**2\_Erste Schulung:** Nach der Kampagne durchlaufen die Mitarbeiter das erste Schulungsmodul auf unserer eLearning Plattform und erhalten nach erfolgreichem Abschluss eines kurzen Quiz ein Zertifikat.

**3\_Zweite Schulung:** Nach mehreren Monaten schalten wir ein weiteres Schulungsmodul frei, welches die Mitarbeiter erfolgreich abschließen müssen.

**4\_Auswertung des Erfolgs:** Innerhalb von 12 Monaten erfolgt die zweite Managed Phishing Kampagne zur Überprüfung des Erfolgs der bisherigen Maßnahmen.

**42 Mrd.**

**SPAM-Mails**

**55 Mrd. Schadens-**  
**summe, 50 % aller**

**Unternehmen betroffen**

**92% der Cyberattacken**  
**per E-Mail**

**Wir beraten Sie gerne und machen Ihnen ein Angebot  
passend zu Ihrer individuellen Unternehmensstruktur.**

**Mit uns zur Top-Informationssicherheit**



 **ADICOM<sup>4.0</sup>**