

# Security Awareness Service



## 1. Der Security Awareness Service

» **Möchten Sie als Mitarbeiter für einen Phishing-Angriff im Unternehmen verantwortlich sein?** «

Die Sicherheit der Unternehmensdaten und -systeme hat oberste Priorität. Die wachsende Zahl und Professionalität von Cyber-Bedrohungen erfordern ein hohes Maß an Aufmerksamkeit von uns allen. Der Mensch ist und bleibt die erste und wichtigste Verteidigungslinie gegen Angriffe von außen. Einzelne Sicherheitsvorfälle, oft durch gezielte Angriffe wie Phishing ausgelöst, können schwerwiegende finanzielle und rufschädigende Konsequenzen haben.

Um das Sicherheitsbewusstsein im gesamten Unternehmen proaktiv zu schärfen und zu vereinheitlichen, implementieren wir einen automatisierten Security Awareness Service von Hornetsecurity. Dieser soll Sie dabei unterstützen, potenzielle Gefahren frühzeitig zu identifizieren und angemessen darauf zu reagieren.

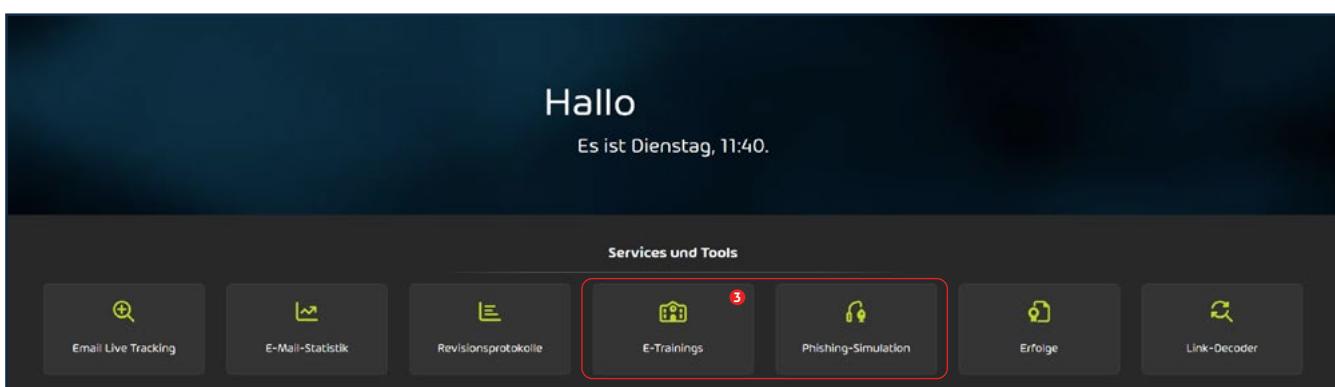
Ein Herzstück dieses Services ist die Phishing-Simulation, bei der wir Ihnen E-Mails zusenden, die reale Angriffe nachahmen. Hierbei geht es ausschließlich um Ihr Training: Sollten Sie auf einen Link oder Anhang klicken, werden Sie umgehend auf eine sichere Seite weitergeleitet. Dort zeigen wir Ihnen konkret die Merkmale, an denen Sie die gefälschte E-Mail hätten erkennen können. Ergänzt durch kurze Trainingsmodule, bereiten diese praktischen Übungen Sie effektiv auf den Ernstfall vor. So lernen Sie ohne jedes Risiko, reale Bedrohungen souverän zu erkennen und schützen damit aktiv das Unternehmen und Ihre Daten.

In dieser Anleitung erklären wir Ihnen den Umgang mit dem Service.

## 2. Das User Panel

Melden Sie sich in Ihrem persönlichen Dashboard mit Ihrer E-Mail-Adresse und Ihrem Passwort an:  
[https://cp.hornetsecurity.com/user\\_dashboard](https://cp.hornetsecurity.com/user_dashboard)

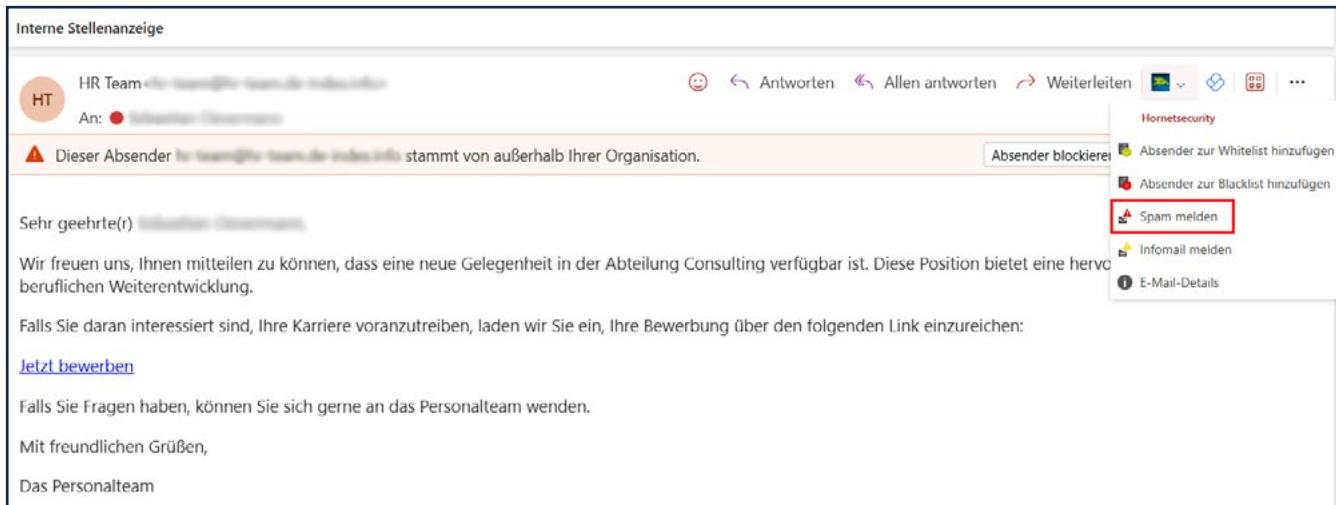
Für den Security Awareness Service sind die beiden Punkte „E-Trainings“ und „Phishing-Simulation“ wichtig.



### 3. Phishing-Simulation

Der wichtigste Bestandteil des Security Awareness Service ist die Phishing-Simulation. Sie werden in der nächsten Zeit Mails bekommen, die versuchen werden, Sie auf verschiedenste Weisen reinzulegen.

Eine beispielhafte Phishing-Mail könnte wie folgt aussehen:



The screenshot shows an email in the inbox with the following details:

- From:** HR Team <no-reply@soeaweb.de>
- To:** [redacted]
- Subject:** Interne Stellenanzeige
- Message Content:**

Dieser Absender <no-reply@soeaweb.de> stammt von außerhalb Ihrer Organisation.

Sehr geehrte(r) [redacted]

Wir freuen uns, Ihnen mitteilen zu können, dass eine neue Gelegenheit in der Abteilung Consulting verfügbar ist. Diese Position bietet eine hervorragende berufliche Weiterentwicklung.

Falls Sie daran interessiert sind, Ihre Karriere voranzutreiben, laden wir Sie ein, Ihre Bewerbung über den folgenden Link einzureichen:

[Jetzt bewerben](#)

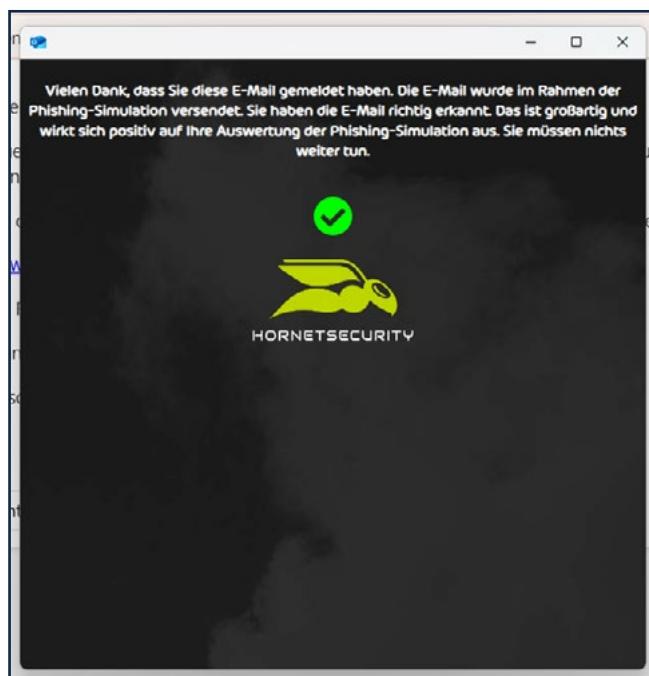
Falls Sie Fragen haben, können Sie sich gerne an das Personalteam wenden.

Mit freundlichen Grüßen,

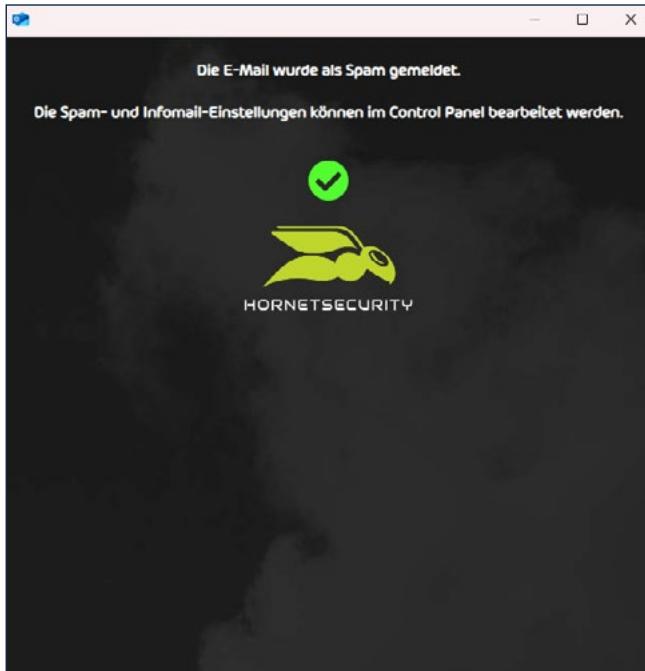
Das Personalteam
- Actions (on the right):**
  - Absender blockieren
  - Hornetsecurity (dropdown menu)
    - Absender zur Whitelist hinzufügen
    - Absender zur Blacklist hinzufügen
    - Spam melden** (highlighted with a red box)
    - Infomail melden
    - E-Mail-Details

Wenn Sie die Mail als Phishing identifizieren, müssen Sie die Mail über den Button von Hornetsecurity auf der rechten Seite als Spam melden.

Nach dem Melden erscheint ein Fenster mit der Info, ob es sich um eine Mail der Phishing-Simulation handelt:



Wenn es sich bei der von Ihnen gemeldeten Mail nicht um eine Mail der Phishing-Simulation handelt, erscheint das folgende Fenster und die Mail wird zur Prüfung an den Anbieter gesendet.



## 4. E-Trainings

Unter „E-Trainings“ finden Sie Ihre offenen und abgeschlossenen Trainings. Die Zahl drei markiert, dass drei Trainings noch offen sind und daher zeitnah durchgeführt werden sollten.

The screenshot displays the SAS E-Training platform. At the top, there is an info message: "Sie können ein E-Training starten, indem Sie darauf klicken. Ihr Fortschritt wird automatisch gespeichert. Sie können das E-Training jederzeit unterbrechen und später fortsetzen. Das Symbol oben rechts zeigt den Trainingsstatus des E-Trainings. Wir empfehlen Ihnen, Kopfhörer oder Lautsprecher zu verwenden. Alternativ können Sie im Programm Untertitel einschalten." Below this is a search bar labeled "Suchen".

**Anstehende E-Trainings:** This section lists three open trainings:

- Quiz: Social Engineering (6m ago)
- Quiz: Soziale Medien (4m ago)
- Willkommen bei SAS (5m ago)

**Abgeschlossene E-Trainings:** This section lists four completed trainings, each with a "Bitte bewerten Sie dieses E-Training" button:

- Phishing-Einführung (6m ago)
- Gefährliche Makros – Emotet und die Makrovirenpandemie (1m ago)
- Sich gegen Phishing-Angriffe schützen (6m ago)
- Social Engineering (8m ago)

Zusätzlich bekommen Sie bei offenen Trainings alle 30 Tage eine E-Mail als Erinnerung zugesendet:



A screenshot of an email titled "Einladung zum E-Training". The email is from "Mein Austing - Office &amp; E-Mail-Security&lt;noreply@austing.it.de&gt;" with the subject "An: Sie". The body of the email includes the "austing." logo, a title bar "Einladung zum E-Training", and text about available training modules and completed ones. It ends with a friendly greeting from "große Austing GmbH".

Je mehr Mails Sie erfolgreich erkennen und je mehr E-Trainings Sie durchführen, desto schwieriger werden die Mails.

Unter „Phishing-Simulation“ können Sie Ihre Auswertung der Phishing-Mails einsehen:

A screenshot of a web-based phishing simulation dashboard. It shows sections for "PHISHING-SIMULATION" (with a note about reporting received emails), "Gut zu wissen" (information about simulated emails from colleagues), "ZU IHREN EINSTELLUNGEN GEHEN" (link to settings), "AUSWERTUNG DER PHISHING-SIMULATION" (a donut chart showing 26 total emails: 100% recognized, 0% reported, 0% fallen for), and "MANIPULATIVE TRICKS" (a note about manipulative tricks and a link for more information). A success message at the bottom states "Sehr gut, Sie sind bislang noch auf keinen manipulativen Trick hereingefallen, wie z. B. Zeitdruck, Autorität oder Neugier."

## 5. Gezielte Unterstützung:

Unsere zusätzlichen Schulungsoptionen

Unser Security Awareness Service ist die ideale Basis, um die allgemeine Sicherheit zu stärken. Oft ist es auch sinnvoll, für eine Gruppe von Mitarbeitern Schulungen durchzuführen, die gezielt auf sie zugeschnitten sind. In diesem kleineren, persönlichen Rahmen gehen wir auf individuelle Fragen ein und arbeiten gemeinsam praxisnahe Szenarien durch.

Melden Sie sich unter der Telefonnummer 04442 / 9264 54 oder der [consulting@austing-it.de](mailto:consulting@austing-it.de), wenn Sie für Ihr Unternehmen oder Ihre Abteilung einen solchen Bedarf sehen. Wir finden dann die beste Lösung, um die Sicherheit gezielt bei Ihnen zu festigen. Informieren Sie sich auch gerne über unsere weiteren Schulungsangebote unter: <https://www.austing-it.de/schulung-weiterbildung>

## Ihr Ansprechpartner:



**Sebastian Oevermann**  
Consultant  
Informationssicherheitsbeauftragter - Microsoft Certified  
 [s.oevermann@austing-it.de](mailto:s.oevermann@austing-it.de)  
 04442 9264 54