

E-Mail-Sicherheit / HornetSecurity / Security Awareness Service / Ablauf und Reaktionen

Kurzbeschreibung: Was passiert beim aktivierten Security Awareness Service, wenn eine simulierte Phishing-E-Mail zugestellt wird? Dieser Artikel erklärt den Ablauf, die verschiedenen Reaktionsmöglichkeiten und wie sich das persönliche Level dadurch verändert.

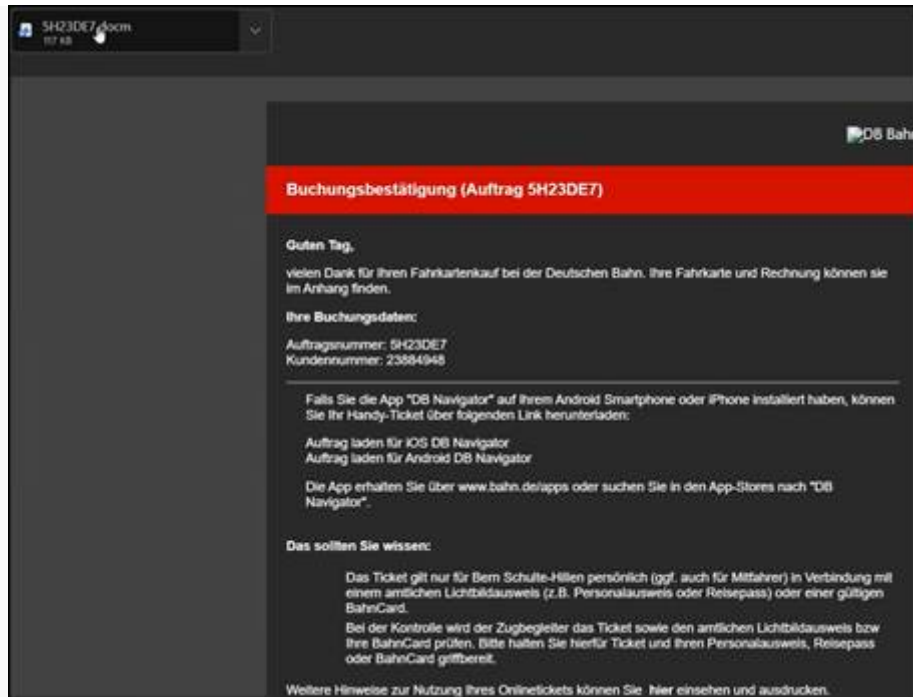
Für wen relevant?

- Alle Mitarbeiter, deren Postfach über den HornetSecurity Security Awareness Service abgesichert wird und die simulierte Phishing-Mails erhalten.

Kurze Erklärung – Wie funktioniert der Security Awareness Service?

- Der Security Awareness Service arbeitet mit verschiedenen **Leveln**. Jeder Benutzer beginnt in Level 1, dem niedrigsten Level, und steigt oder fällt je nach Reaktion auf simulierte Phishing-E-Mails.
- Ein Aufstieg ist möglich, wenn verdächtige E-Mails erkannt und über das HornetSecurity-Add-in in Outlook gemeldet werden. Je höher das Level, desto anspruchsvoller werden die simulierten Phishing-Mails.
- Grundlage dafür ist der **Employee Security Index (ESI®)** von HornetSecurity, ein Benchmark, der das Sicherheitsverhalten fortlaufend misst und daraus steuert, welche Trainingsinhalte und wie anspruchsvolle Phishing-Simulationen als Nächstes zugestellt werden.





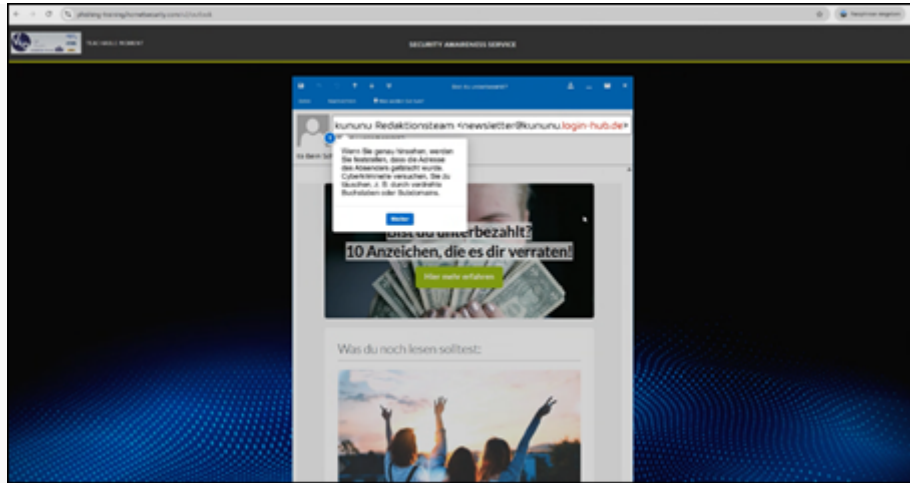
Wie wirken sich verschiedene Reaktionen aus?

Der Benutzer kann mit der Phishing-E-Mail wie mit jeder E-Mail interagieren – beispielsweise den Anhang öffnen oder auf enthaltene Links klicken.

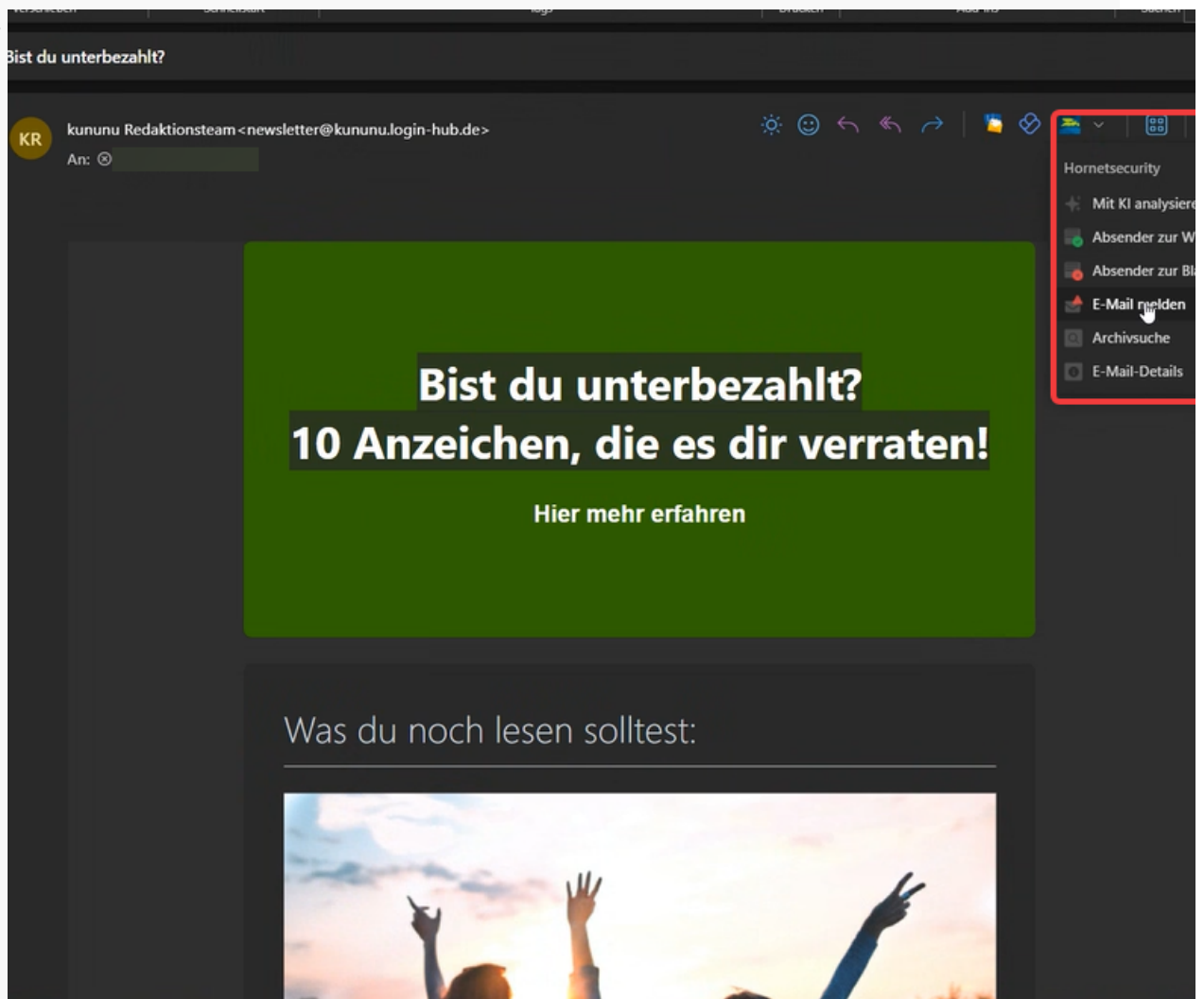
1. **Interaktion mit der Mail (Anhang öffnen, Link klicken):** Es wird ein Hinweisfenster eingeblendet, das informiert, dass es sich um eine Phishing-Mail handelt.

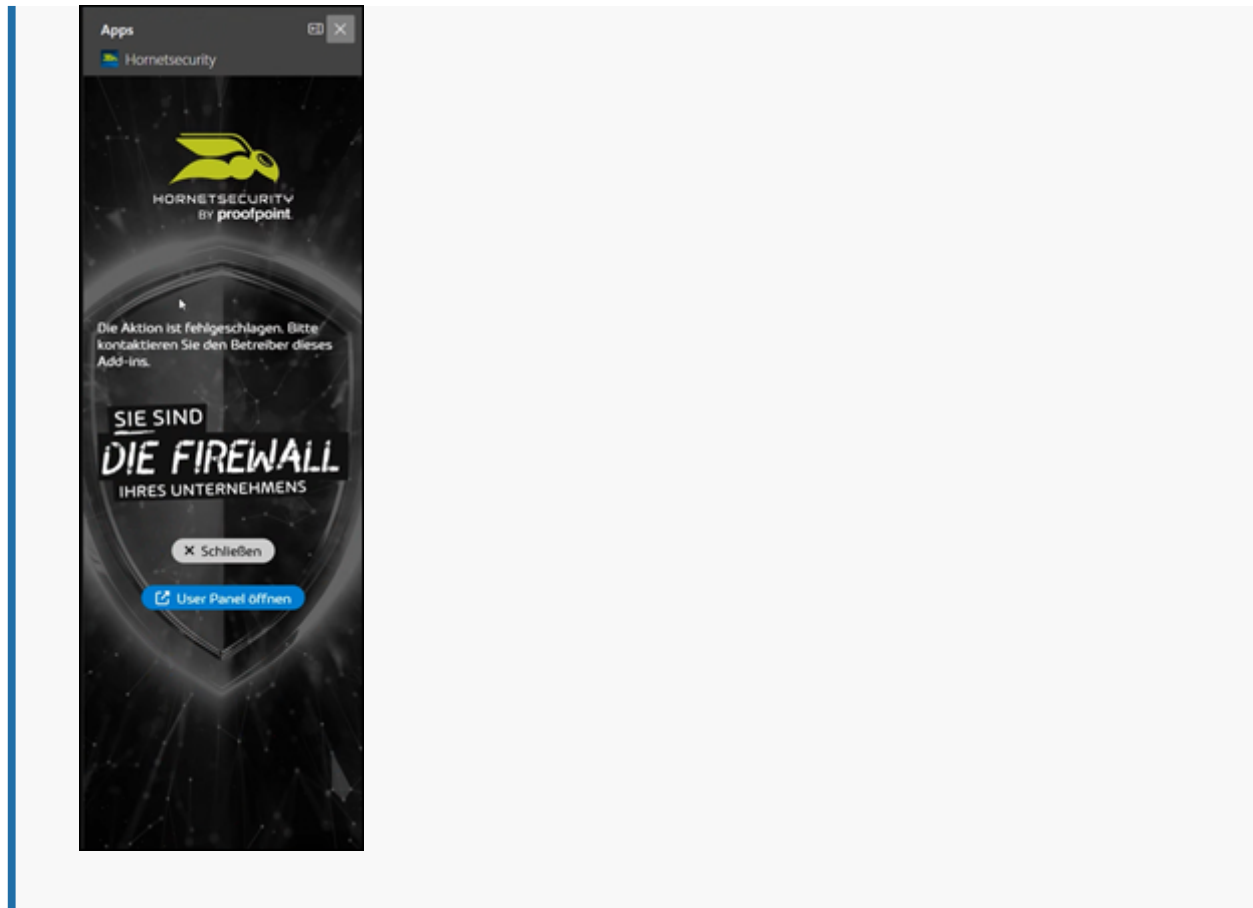


2. Nach einer solchen Interaktion kann direkt ein sogenannter **Teachable Moment** angezeigt werden. Diese E-Trainings beziehen sich unmittelbar auf die zuvor ausgelöste Phishing-Mail und unterstützen den Lernprozess.



3. **Korrektes Melden:** Alternativ kann die E-Mail über das HorneSecurity-Outlook-Add-in gemeldet werden. Wird eine E-Mail korrekt gemeldet, erhält der Benutzer umgehend eine Rückmeldung.





4. **Ignorieren:** Eine weitere Möglichkeit besteht darin, die E-Mail zu ignorieren.

Hinweis Sowohl durch korrektes Melden als auch durch Ignorieren steigt der Benutzer schrittweise im Level auf. Das Ignorieren der Mails hat jedoch nicht den gewünschten Effekt – erst das aktive Erkennen und Melden trainiert den sicheren Umgang mit echten Phishing-Angriffen nachhaltig.

Achtung Nicht jede Interaktion wird gleich bewertet: Das Öffnen potenziell gefährlicher Inhalte (z. B. eine Makrodatei im Anhang) wird deutlich negativer gewertet als das bloße Öffnen einer E-Mail. Bei schwächerem Sicherheitsverhalten kann das Level daher auch wieder sinken und die Simulationen werden vorübergehend wieder einfacher, bis sich das Verhalten verbessert.

Tipp Verdächtige E-Mails können nicht nur über das Outlook-Add-in gemeldet werden, sondern in vielen Konfigurationen zusätzlich per Weiterleitung an die Adresse reportto@hornetsecurity.com. Welcher Weg für Ihr Unternehmen zur Verfügung steht, teilt Ihnen bei Bedarf Ihr IT-Team mit.

Kurze Checkliste

- Wissen, dass alle Benutzer in Level 1 starten und sich das Level durch das eigene Verhalten verändert?
- Bei einer verdächtigen (simulierten) Phishing-Mail: nicht interagieren, sondern über das HornetSecurity-Add-in melden?
- Teachable Moments/E-Trainings nach Interaktion mit einer simulierten Phishing-Mail bewusst durcharbeiten?

- Bewusst, dass reines Ignorieren zwar zum Levelaufstieg beiträgt, aber weniger effektiv trainiert als aktives Melden?

FAQ – kurz & knapp

- Was passiert, wenn ich auf eine simulierte Phishing-Mail hereinfalle?
 - Es erscheint ein Hinweisfenster, das über die Simulation aufklärt, häufig gefolgt von einem kurzen, auf den Vorfall zugeschnittenen E-Training (Teachable Moment).
- Wie steige ich im Level auf?
 - Durch korrektes Erkennen und Melden simulierter Phishing-Mails über das HornetSecurity-Add-in – aber auch durch bloßes Ignorieren steigt das Level, wenn auch mit geringerem Lerneffekt.
- Kann mein Level auch wieder sinken?
 - Ja, insbesondere bei riskanteren Interaktionen wie dem Öffnen potenziell gefährlicher Anhänge wird das Sicherheitsverhalten negativer bewertet, was sich auch auf das Level auswirken kann.
- Was ist der Employee Security Index (ESI®)?
 - Ein von HornetSecurity entwickelter Benchmark, der das Sicherheitsverhalten von Mitarbeitenden fortlaufend misst und daraus ableitet, welche Trainingsinhalte und Phishing-Simulationen als Nächstes sinnvoll sind.

Fußzeile

Bei der Erstellung von BranchXStack-Inhalten kann auch KI zum Einsatz kommen. Alle Inhalte werden jedoch redaktionell von Menschen geprüft und bei Bedarf überarbeitet.

Shortlink: <https://csg.gmbh/faq-hornetsecurity-awareness-ablauf>

Created 2026-07-31 06:00:45 UTC by CSGJRAdmin

Updated 2026-07-31 06:03:26 UTC by CSGJRAdmin