DIGITALEDENKART

Managed Services

# Ankündigung SAS

## Marken

Produktnamen werden nur zur Identifikation der Produkte verwendet und können eingetragene Marken der entsprechenden Hersteller sein.

## Eigentumshinweis

Anwendungseinschränkungen und Offenlegung der Vorschlags- und Angebotsdaten.

Die in diesem Vorschlag bzw. Angebot auf allen Seiten enthaltenen Informationen (Daten) sind Unternehmensgeheimnisse und/oder unternehmensinterne bzw. finanzielle Informationen, die vertraulich oder nur für einen bestimmten Personenkreis vorgesehen sind. Sie werden unter der Voraussetzung der Geheimhaltung zur Verfügung gestellt und dürfen nicht ohne Genehmigung des Bevollmächtigten zu anderen Bewertungszwecken verwendet oder offen gelegt werden. Kommt jedoch ein Auftrag auf Basis dieses Vorschlages bzw. Angebots zustande, hat der Kunde das Recht, diese Informationen (Daten) in dem im Vertrag festgelegten Umfang zu verwenden und offen zu legen. Diese Einschränkung bezieht sich nicht auf das Recht vom Kunden diese Informationen (Daten) zu verwenden oder offen zu legen, wenn sie von einer anderen Quelle ohne Einschränkung zur Verfügung gestellt werden.

## Revision

| lfd. Nr. | Bemerkung | Datum | Mitarbeiter |
|---|---|---|---|
| 1 | Erstellung Dokument | 21.07.2025 | LB |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

# Inhalt

# 1. Die interne Ankündigung

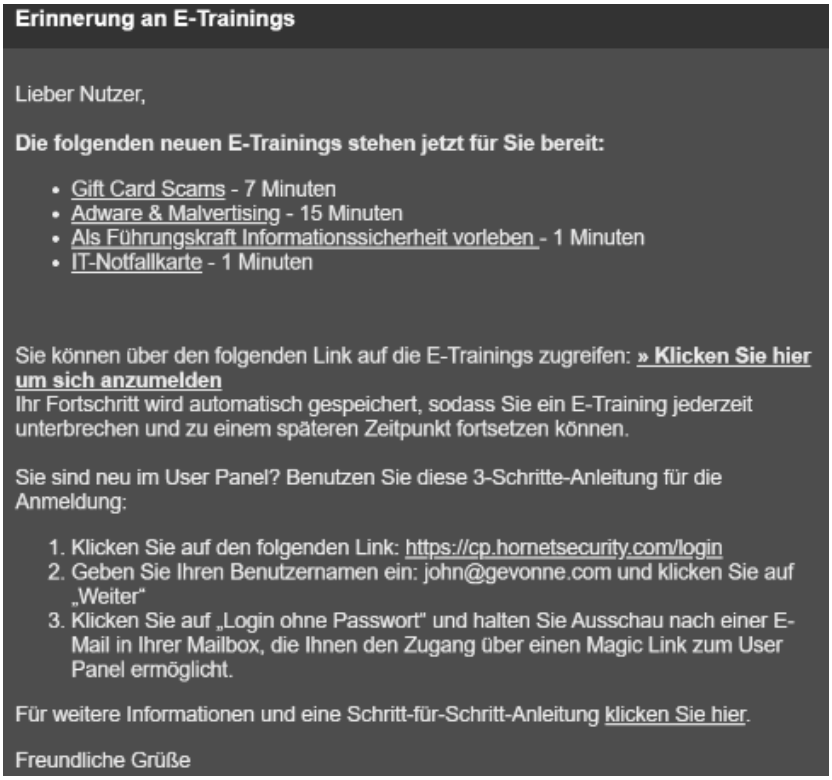
Wir empfehlen, die Benutzer im Vorfeld per E-Mail über den Security Awareness Service zu informieren.

## 1.1 Zeitpunkt der internen Ankündigung

Die Ankündigung sollte ungefähr eine Woche vor dem Projektstart an die Benutzer gesendet werden. Dadurch ist der Abstand zwischen der Ankündigung und dem Versand der ersten Phishing-E-Mails für die Benutzer groß genug, sodass sie in ihrem Alltag nicht mehr an die bevorstehende Phishing-Simulation denken. Dadurch fallen die Benutzer leichter auf die simulierten Phishing-Angriffe herein.

## 1.2 Folgen bei keiner internen Ankündigung

Die Benutzer sind nicht über das Projekt informiert, was zum einen zu Unzufriedenheit der Benutzer führen kann, weil sie sich hintergangen und kontrolliert fühlen. Zum anderen klicken die Benutzer eventuell aus Neugier auf die Links in den E-Mails, obwohl sie die E-Mail als Phishing identifiziert haben, und verfälschen so die Ergebnisse. Auch E-Training Einladungen können ignoriert werden, wenn die Mitarbeiter nicht vorab informiert wurden. Das folgende Bild ist ein Beispiel einer möglichen E-Training-Einladung, die Benutzer erhalten können.



**Erinnerung an E-Trainings**

Lieber Nutzer,

**Die folgenden neuen E-Trainings stehen jetzt für Sie bereit:**

- Gift Card Scams - 7 Minuten
- Adware & Malvertising - 15 Minuten
- Als Führungskraft Informationssicherheit vorleben - 1 Minuten
- IT-Notfallkarte - 1 Minuten

Sie können über den folgenden Link auf die E-Trainings zugreifen: **» Klicken Sie hier um sich anzumelden**
Ihr Fortschritt wird automatisch gespeichert, sodass Sie ein E-Training jederzeit unterbrechen und zu einem späteren Zeitpunkt fortsetzen können.

Sie sind neu im User Panel? Benutzen Sie diese 3-Schritte-Anleitung für die Anmeldung:

1. Klicken Sie auf den folgenden Link: https://cp.hornetsecurity.com/login
2. Geben Sie Ihren Benutzernamen ein: john@gevonne.com und klicken Sie auf „Weiter"
3. Klicken Sie auf „Login ohne Passwort" und halten Sie Ausschau nach einer E-Mail in Ihrer Mailbox, die Ihnen den Zugang über einen Magic Link zum User Panel ermöglicht.

Für weitere Informationen und eine Schritt-für-Schritt-Anleitung klicken Sie hier.

Freundliche Grüße

# 2. Vorlage interne Ankündigung

Liebe Kolleginnen und Kollegen,

die Gewährleistung der IT-Sicherheit stellt Unternehmen vor immer größere Herausforderungen. Während Privatanwender besonders von der Nutzung veralteter Software und Spam gefährdet werden, haben Unternehmen insbesondere mit „digitaler Sorglosigkeit" und daraus resultierendem Fehlverhalten im Alltag zu kämpfen.

Wir haben uns daher entschlossen, in Zusammenarbeit mit der Digitale Denkart Managed Services GmbH eine Schulung zu Themen der IT-Sicherheit durch den Security Awareness Service durchzuführen und bauen dabei auf Ihre Mitarbeit. Im Rahmen einer Phishing-Simulation werden E-Mails an die teilnehmenden Benutzer versendet, um aktuelle Phishing-Angriffe zu simulieren und etwaiges Fehlverhalten wie das Öffnen eines Links oder eines Dateianhangs zu provozieren. Dabei geht es um Ihr Training: Nach einem potenziell gefährlichen Klick werden Sie zu einer interaktiven Erklärseite geleitet. Dort wird aufgezeigt, wie Sie die gefälschte E-Mail hätten enttarnen können.

Im Rahmen der Maßnahme werden auch E-Mails im Namen von Kolleg*innen gesendet: Sie können also auch Absender einer solchen simulierten Phishing-E-Mail sein. In Ihrem User Panel (https://cp.digitaledenkart.de/usersettings/settings) haben Sie die Möglichkeit, diesem Vorgehen zu widersprechen.

Die im Rahmen des Trainings gewonnenen Daten werden anonymisiert und gruppenbasiert ausgewertet, es kann an keiner Stelle Rückschluss auf Ihr persönliches Klickverhalten gezogen werden. Nach Abschluss der Auswertung wird jeglicher Bezug zu Benutzern gelöscht.

Wir bedanken uns für Ihre Unterstützung!