DIGITALEDENKART

Managed Services

Awareness Maßnahmen

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. Awareness Maßnahmen

Im Rahmen des Aufbaus einer Sicherheitskultur in Bezug auf die Cyber-Security werden Ihnen Phishing-Simulationen sowie E-Learnings zu Verfügung gestellt.

Phishing gehört zu einer weitverbreiteten Maßnahme von Cyber-Kriminellen. Hierbei werden gefälschte Mails versendet, die dazu verleiten sollten auf einen Betrug hereinzufallen. Die Angreifer zielen darauf ab verschiedene Informationen, wie Finanzdaten, Zugangsdaten oder andere sensible Daten von den Nutzern zu erhalten.

1.1 Phishing-Simulationen

Die Phishing-Simulationen sind realitätsnah aufgebaut und simulieren die Vorgehensweise echter Angreifer. Hier enthalten sind unter anderem verschiedene psychologische Manipulationsfaktoren.

Mit Hilfe der Simulationen fällt es Ihnen künftig leichter die echten Phishing-Mails zu erkennen.

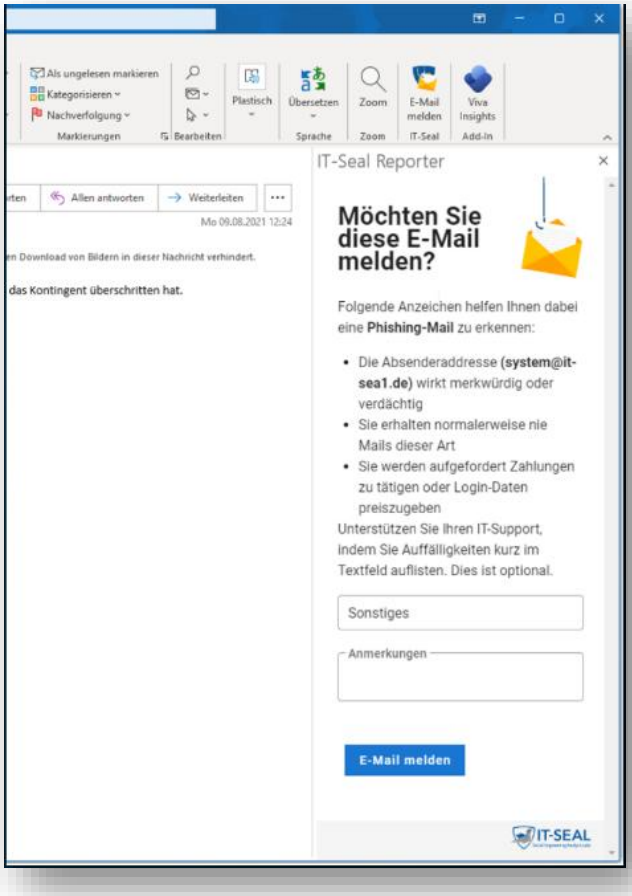
1.1.1. Reporterbutton

Der Reporter-Button ist in Ihrer Menüleiste in Outlook automatisch von Ihrem Administrator der Digitale Denkart Managed Services GmbH integriert worden.

<u>Der Reporterbutton:</u>

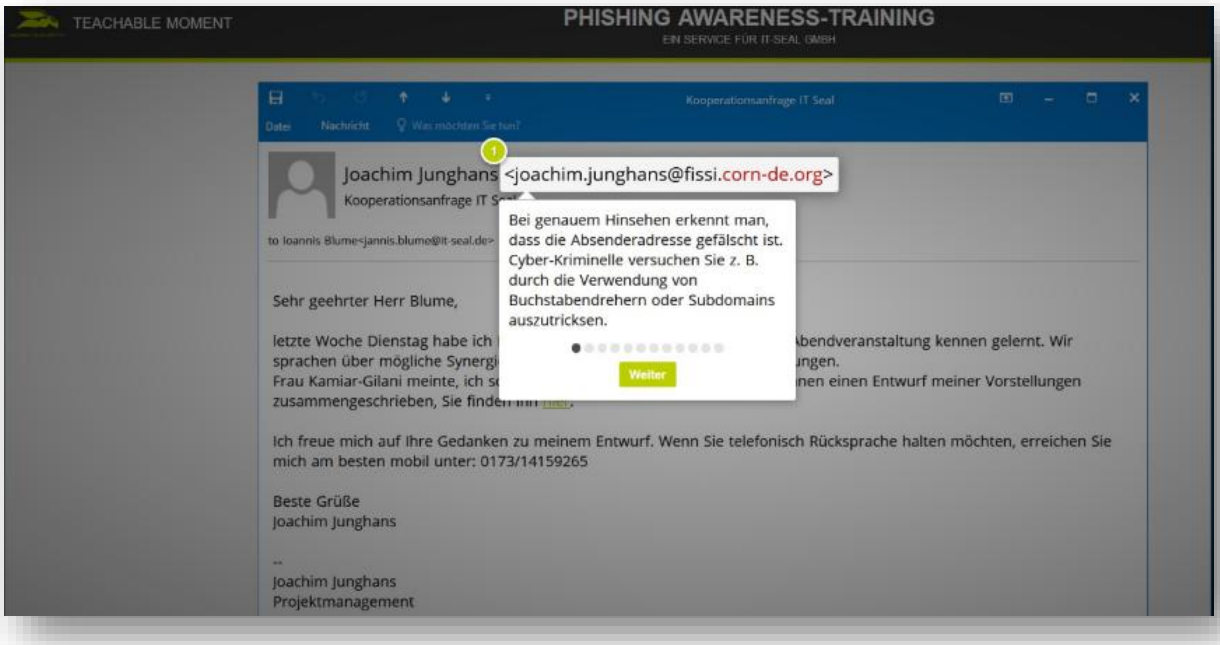
Wenn Sie eine simulierte Phishing-Mail erhalten und diese erkennen, können Sie diese Mail in Outlook auswählen und mit einem Klick auf dem Reporterbutton diese Mail melden.

Sie erfahren im Nachgang dann, ob es sich wirklich um eine simulierte Phishing-Mail gehandelt hat.



1.1.2 Most Teachable Moment

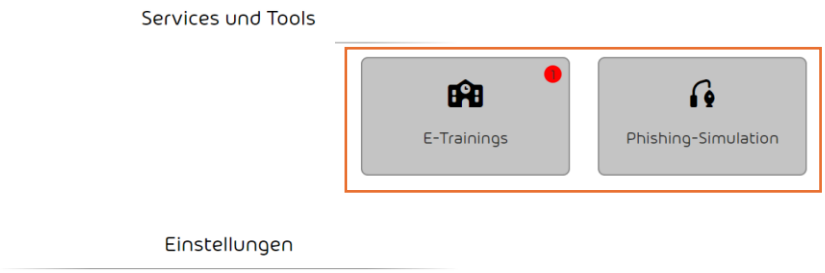
Sollten Sie eine Phishing-Simulation nicht rechtzeitig erkannt haben und etwa beispielsweise ein enthaltenes Word-Dokument oder einen Link geöffnet haben, werden Sie anhand des „Most-Teachable-Moment“ hierauf hingewiesen. In wenigen Minuten werden Ihnen die Hinweise gezeigt, welche diese Phishing-Mail verraten hätten und worauf nun verstärkt geachtet werden kann.



2. User Panel

Im User Panel ist Ihre persönliche Lernplattform enthalten. Hier erhalten Sie eine Übersicht über die E-Learnings sowie Phishing-Simulationen. Den Zugangslink zu Ihrem Security-Hub haben Sie bereits per Mail erhalten. Es empfiehlt sich, sich den Link als Favorit im Browser Ihrer Wahl abzuspeichern.

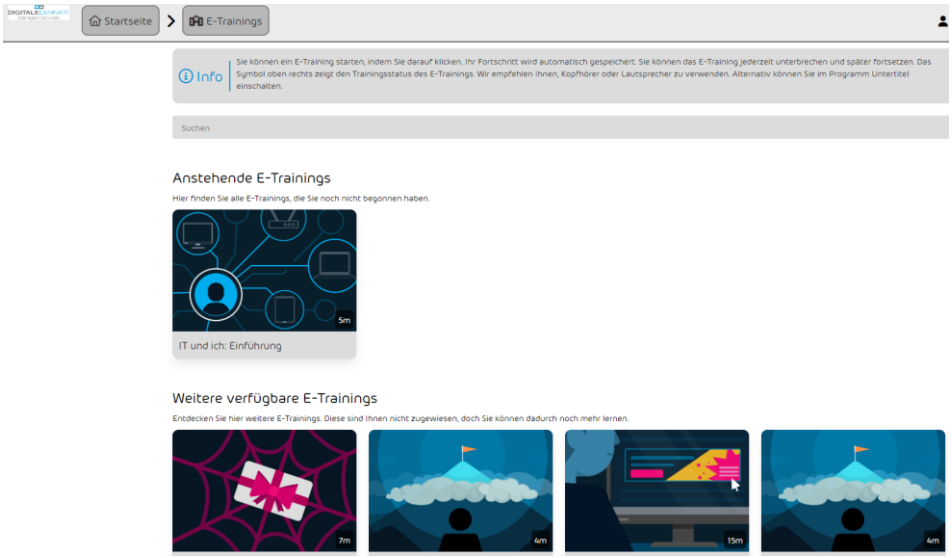
Link: https://cp.digitaledenkart.de/



2.1 E-Learnings

In regelmäßigen Abständen werden neue E-Learnings im User Panel - Modul E-Learnings bereitgestellt. Hier halten Sie dann eine Info-Mail, dass neue Lerninhalte verfügbar sind. Sollten Sie nach 2-4 Wochen das neue E-Learning nicht durchgeführt haben, erhalten Sie eine Erinnerungsmail.

Die E-Learnings sind so ausgelegt, dass sie sich einfach in den Alltag integrieren lassen und umfassen nur wenige Minuten. Im Security-Hub sehen Sie sowohl die neuen Lerninhalte wie auch bereits abgespielte E-Learnings. Diese können Sie gerne wiederholen.



2.2 Phishing-Simulationen

Im User Panel unter dem Modul Phishing E-Mails sehen Sie alle Phishing-Mails, welche Ihnen bereits zugesendet wurden, sowie eine Statistik Ihrer empfangenen Phishing-Simulationen. Hier ist enthalten, welche Sie als solche erkannt haben und welche nicht. Sie können Sie hier ebenfalls nochmal ansehen, woran Sie die Phishing-Mail erkennen können, und welche emotionalen Absichten der Angreifer hierbei hatte.