fake phishing mail service
&
cybersecurity awareness training

CAT

-REALISIERUNG & DURCH-FÜHRUNG-

Auftraggeber	Marc Aeby
Projektleiter	J. Storrer
Autor	J. Storrer
Dokument	ID2132_StorrerJessica_FPM&CAT_Studie.docx
Klassifizierung	Intern
Status	Genehmigt

Änderungsverzeichnis

Datum	Version	Änderung	Autor
01.12.2023	0.1	Erster Draft	J. Storrer
12.12.2023	0.2	Diverse Änderungen	J. Storrer
14.12.2023	1.0	Final Dokument	J. Storrer

Inhaltsverzeichnis

Inhaltsverzeichnis 1
Abbildungsverzeichnis 3
Tabellenverzeichnis 5
1. Marketing 6
1.1 Zielgruppen 6
1.2 Unique Selling Proposition (USP) 6
1.3 Marketing-Kanäle 6
1.4 Angebotsstruktur 7
1.5 Erfolgsmessung 7
2. ROI 8
2.1 Plattform- & Kurserstellungskosten 8
2.2 ROI-Berechnung 8
2.3 Break Even 9
2.4 Schlussfolgerung 9
2.5 Massnahmen 9
3. MINI BUSINESS CASE 10
3.1 Einführung 10
3.2 Geschäftsgelegenheit 10
3.3 Lösung 10
3.4 Finanzanalyse 10
3.5 Umsetzungsplan 11
3.5.1 Phasen 11
3.6 Risiken und Mitigation 11
3.7 Abschluss 12
4. Fact Sheet 13
4.1 Überblick und Beschreibung des Services 13
4.2 Zielgruppe des Services: 13
4.3 Service-Eigenschaften 13
4.4 Service Level Agreements (SLAs): 13
4.5 Sicherheitsmerkmale und Compliance-Informationen: 13
4.6 Technische Details 14
4.6.1 Plattformen und Technologien: 14
4.6.2 Integration mit anderen Services und Systemen: 14
4.7 Kosten und Preismodell 14
4.7.1 Kostenstruktur: 14
4.7.2 Mögliche Rabatte oder Staffelpreise: 14
4.8 Support- und Kontaktinformationen 14
4.8.1 Erreichbarkeit des Supports: 14
4.9 Eskalationsprozeduren und wichtige Kontaktpersonen: 15
4.10 Nutzungsstatistiken und Performance-Indikatoren 15
4.11 Zugriff und Berechtigungen 15
4.12 Implementierungs- und Migrationsdetails 15
4.12.1 Schritte zur Einführung des Services für neue Nutzer: 15
4.12.2 Dokumentation und Schulungsressourcen 15
4.13 Geplante Erweiterungen oder Verbesserungen: 15
5. Testcases 16
6. Ausführung 17
6.1 MJCS – mjcyberseucrity.com 17
6.1.1 Startseite (Homepage) 19

6.1.2 Weitere Bereiche 21
6.2 CAT – mjcybersecurity.teachable.com 28
6.3 Woche 1: Phishing Mail: Erkennen & Handeln 30
6.3.1 TAG 1 (Tag 1): Einführung & Einführung in Phishing-Mails 30
6.3.2 TAG 2 (Tag 2): Phishing-Mails erkennen 31
6.3.3 TAG 3 (Tag 3): Fallstudien und Praxisbeispiele 31
6.3.4 TAG 4 (Tag 4): Melden und Handeln bei Phishing-Mails 32
6.3.5 TAG 5 (Tag 5): Zusammenfassung des Kurses 32
6.3.6 Eindrücke vom Kurs Woche 1 – Phishing Mails: Erkennen & Handeln 33
6.4 Woche 2: Wissen wie der Hacker denkt: Audioexkurs zu Social Engineering 46
6.4.1 TAG 1 Social Engineering: Vertrauen und Autorität 46
6.4.2 TAG 2 Social Engineering: FOMO & Dringlichkeit & Knappheit 46
6.4.3 TAG 3 Social Engineering: Gegenseitigkeit & Norm der Gegenseitigkeit (Reziprozität) 46
6.4.4 TAG 4 Social Engineering: Emotionale Manipulation 46
6.4.5 Zusatz - TAG 5: Achtsamkeit 46
6.4.6 Einblicke Woche 2 Wissen wie der Hacker denkt: Audioexkurs zu Social Engineering 47
6.5 Woche 3: IT-Sicherheit am Arbeitsplatz 56
6.5.1 TAG 1: Einführung in IT-Sicherheit am Arbeitsplatz 56
6.5.2 TAG 2: Passwortsicherheit 56
6.5.3 TAG 3: Sicheres Arbeiten im WWW 56
6.5.4 TAG 4: Sicherheitsrichtlinien und Best Practices 56
6.5.5 TAG 5: Zusammenfassung Woche 3 56
6.5.6 Eindrücke in den Kurs 57
6.6 CAT-Teachable MJCS Pages 70
6.7 Digitale Downloads 70
6.8 Sales-Pages 71
6.9 Achtsamkeits Zusatz 71
6.10 CAP (Zusatz) 72
6.11 Backend 72
6.11.1 Dashboard & Auswertungen 72
7. Abschlussworte Realisierung 75
Literaturverzeichnis 76
Eidesstattliche Erklärung 77

Abbildungsverzeichnis

Abbildung 1 - Home mjcybersecurity.com 17
Abbildung 2 - Anpreisung Services auf mjcybersecurtiy.com.....18
Abbildung 3 - weitere Anpreisung des Services.....19
Abbildung 4 - FPM-Site von mjcybersecurity.com 21
Abbildung 5 - Weitere FPM-Service Details.....22
Abbildung 6 - FPM-Reportbeispiel für Kunden.....23
Abbildung 7 - How To CAT.....24
Abbildung 8 - WhitePaper/FactSheet/KundenonboardingBeispiel Download pro Service 24
Abbildung 9 - QR-Phishing.....25
Abbildung 10 - Oopsie Page B&T AG.....26
Abbildung 11 - Über uns.....27
Abbildung 12 - Footer.....28
Abbildung 13 - Einstiegsseite CAT auf Teach:able.....29
Abbildung 14 - Angebotene Kurse auf Einstiegsseite 30
Abbildung 15 - Einstiegsseite Kurs Woche 1 33
Abbildung 16 - Übersicht Kursplan Woche 1 34
Abbildung 17 - Übersicht Kurs.....35
Abbildung 18 - Mit Timer versehen.....36
Abbildung 19 - Geschichten auch als Audio Verfügbar.....37
Abbildung 20 - Diverse Mini-Games.....38
Abbildung 21 - "How-To" Videos 39
Abbildung 22 - Interaktives Lernen.....40
Abbildung 23 - Div. Praxistipps direkt zum Umsetzen.....41
Abbildung 24 - Hörenverstehen Fallbeispiele 42
Abbildung 25 - Aktuell bleiben.....43
Abbildung 26 - Quizzes 44
Abbildung 27 - Antwortkasten für Feedback.....45
Abbildung 28 - Übersicht Kurs Woche 2.....48
Abbildung 29 - Wie der Kurs funktioniert.....49
Abbildung 30 - Geschichte #1 Woche 2.....50
Abbildung 31 - Geschichte #2 FOMO Woche 2 51
Abbildung 32 - Geschichte #3 Reziprozität Woche 2.....52

Abbildung 33 - Geschichte #4 Auto öffnen lassen Woche 2 53
Abbildung 34 - Zusatz: Atemübung für Achtsam durch den Alltag mit Video 54
Abbildung 35 - MiniGame "Was ist Cybersecurity" 58
Abbildung 36 - Poster Sensible Daten 59
Abbildung 37 - Bildbeispiele "Was DU siehst" & "Was der Hacker sieht" 60
Abbildung 38 - Interaktives Suchspiel "Sicherheitsrisiken" 61
Abbildung 39 - Diverse Antwortkasten 63
Abbildung 40 - Diverse Quizzes 64
Abbildung 41 - Diverse Tipps&Tricks 65
Abbildung 42 - Div. Videos mit Tipps& Tricks 66
Abbildung 43 - Interaktive Zusammenfassungen 67
Abbildung 44 - Big Picture CAT in div. Farben zum Download 68
Abbildung 45 - Digitale Downloads 70
Abbildung 46 - Sales Page "Digitaler Download" 71
Abbildung 47 - Dashboard Teach:able 72
Abbildung 48 – Reportmöglichkeiten 73
Abbildung 49 - Weitere Reportmöglichkeiten pro Kurs 73
Abbildung 50 - Antwortkasten Reports 74

Tabellenverzeichnis

Tabelle 1 - Eindrücke Kurs "Woche 1 Phishing Mails: Erkennen & Handeln".....45
Tabelle 2 - Eindrücke Woche 2: SocialEngineering Audioexkurs.....55
Tabelle 3 - Einblicke in Kurs Woche 3: IT-Security am Arbeitsplatz.....69

1. Marketing

Im folgenden Kapitel wird die Marketing-Strategie aufgezeigt.

1.1 Zielgruppen

Privatpersonen: Personen ohne IT-Hintergrund, die ihre persönlichen Daten besser schützen möchten.

Unternehmen: Firmen, die bereits den Fake Phishing Mail Service nutzen oder an allgemeiner IT-Sicherheit interessiert sind.

1.2 Unique Selling Proposition (USP)

Um den Kurs möglichst so zu gestalten, dass dieser der Teilnehmenden bleibt, wird folgendes umgesetzt.

Praxisorientiertes Lernen: Kursinhalte basieren auf realen Beispielen und wahren Geschichten aus dem Bereich Social Engineering und sind auf alle vier Hauptlerntypen angepasst. Enthält MiniGames, Audios, Fallbeispiele und Videos.

Zwei-in-eins Angebot: Kunden, die den Fake Phishing Mail Service nutzen, erhalten den Kurs kostenlos. Dies fördert die Cross-Selling-Möglichkeiten.

Zusatzmaterialien: Digitale Downloads und Poster mit leicht umsetzbaren Sicherheitstipps zum Ausdrucken und Aufhängen.

Aktuellheit:

Quartalsweise neue Kurse und Digitale Downloads.

1.3 Marketing-Kanäle

Folgende Marketing-Kanäle werden eingesetzt:

E-Mail-Marketing: Versand von personalisierten Angeboten an bestehende Kunden des Fake Phishing Mail Services.

Social Media: Gezielte Kampagnen auf Plattformen wie LinkedIn für professionelles Publikum und Instagramm für Privatpersonen.

POST-Uetendorf: Wochen-Ausstellungsplatz mit Fact-Sheet und Bonus-Coupons wenn in der Geschäftsstelle gesehen.

Content Marketing: Regelmässige Blogbeiträge und Artikel, die die Wichtigkeit von Cybersecurity hervorheben und auf den Kurs aufmerksam machen. Zusatz wie der CAP – Cybersecurity Awareness Podcast.

QR-Code Marketing: Da der QR-Code Fraud steigt, werden QR-Code Kleber überall verteilt, eine Art Gerillia-Werbung, um die Leute Aufmerksam auf Fraud zu machen. Der QR Code führt zu QR | MJCS (mjcybersecurity.com) welche darauf Aufmerksam macht, dass QR Code Phishing am Steigen ist.

1.4 Angebotsstruktur

Folgende Angebotsstruktur wird realisiert werden;

Einführungspreise: Gratisangebote auf Digitale Downloads, Gratis-Kurse für Eng Befreundete. Erste drei Monate 50% Einführungspreis für Privatpersonen.

Gruppenangebote: Rabatte für Unternehmen, die den Kurs für mehrere Mitarbeiter buchen.

1.5 Erfolgsmessung

Die Erfolgsmessung wird mit folgenden zwei Indikatoren Quartalsweise gemessen:

KPIs (Key Performance Indicators):

- Anzahl der Kursanmeldungen
- Umsatzsteigerung durch Cross-Selling mit FPM
- Engagement-Raten bei Social-Media-Kampagnen
- E-Mail-Öffnungsraten.
- Anzahl POST-Kunden

Feedback und Kundenbewertungen: Regelmässige Umfragen zur Kundenzufriedenheit und zur Verbesserung der Kursinhalte.

2. ROI

Es wird von ***150 Kunden pro Quartal*** gerechnet, welche ***je CHF 25.- für einen Kurs*** bezahlen.

2.1 Plattform- & Kurserstellungskosten

Ausgaben

Plattform-, Hosting- & Marketingkosten:

CHF 170 pro Monat für 4 Monate = CHF 680.-

Kurserstellung und -betrieb:

CHF 160 pro Stunde für 15 Stunden = CHF 2'400.- pro Quartal

Gesamtkosten Plattform- & Kursgestaltung:

CHF 680 + CHF 2'400 = CHF 3'080.-

Einnahmen

(Annahme von 150 Kunden im ersten Quartal)

Einnahmen pro Quartal: 150 Kunden * CHF 25 = CHF 3'750

2.2 ROI-Berechnung

Folgend wird mit der folgenden Formel die ROI-Berechung durchgeführt.

$$\text{ROI} = \left(\frac{\text{Einnahmen} - \text{Kosten}}{\text{Kosten}}\right) \times 100$$

Das bedeutet bei den Zahlen:

$$\text{ROI} = \frac{3'750 - 3'080}{3'080} \times 100 = \frac{670}{3'080} \times 100 \approx 21.75\%$$

Wir nehmen die Einnahmen von CHF 3'750 und die Gesamtkosten von CHF 3'080 und berechnen den ROI.

Mit den Kosten ergibt sich ein ROI von etwa 21.75%. Der Service ist profitabel.

2.3 Break Even

Folgend wird der Break-Even auf Kundenanzahl ausgerechnet.

➔ *Bei wievielen Kunden sind die Servicekosten gedeckt?*

$$\text{Anzahl der Kunden} = \frac{\text{Gesamtkosten}}{\text{Preis pro Kunde}}$$

Das bedeutet in Zahlen:

$$\text{Break-Even-Kundenanzahl} = \frac{\text{Gesamtkosten}}{\text{Preis pro Kunde}} = \frac{3'080}{25} \approx 123.2$$

Um die Kosten von CHF 3'080 zu decken, werden ungefähr 124 Kunden pro Quartal benötigt.

2.4 Schlussfolgerung

Der Service ist profitabel, doch eine weitere Steigerung der Rentabilität ist möglich, indem mehr Kunden gewonnen oder der Preis pro Kurs erhöht wird.

2.5 Massnahmen

Effizientere Marketingstrategien, siehe Marketing

3. MINI BUSINESS CASE

Folgend wird ein Mini-Business-Case für den CAT-Service aufgezeigt.

3.1 Einführung

Kurze Beschreibung der Lösung:

Problemstellung: Zunehmende Bedrohung durch Cyberangriffe auf Unternehmen und Privatpersonen.

Lösung: CAT bietet umfassendes Training zur Erhöhung der Sicherheitskompetenz, angeboten über MJ Cybersecurity Services.

3.2 Geschäftsgelegenheit

Folgende Geschäftsgelegenheiten werden für CAT gesehen.

Marktnachfrage: Starkes Wachstum im Bereich der Cybersecurity-Ausbildung, besonders für nicht-technische Nutzer.

Zielgruppe: Privatpersonen und Unternehmen, insbesondere kleine und mittelständische Unternehmen, die ihre Daten und Systeme schützen möchten.

3.3 Lösung

Folgende Lösung wird angeboten

Kursangebot: Online-Training, welche über die Plattform Teachable zugänglich ist. Inhalte umfassen Phishing-Erkennung, Social Engineering und Sicherheitspraktiken am Arbeitsplatz.

Zusatzmaterialien: Digitale Downloads, inklusive Poster mit Sicherheitstipps.

Kostenloser Zugang für bestehende Kunden des Fake Phishing Mail Services.

3.4 Finanzanalyse

Die genau Finanzanalyse kann im Kapitel ROI eingesehen werden.

Einnahmequellen:

Verkauf von Kurslizenzen: Ziel erstes Quartal: 150 Kunden

Preisstruktur: 25 CHF pro Lizenz für Privatpersonen

Kostenstruktur:

Entwicklung: 15h pro Quartal à CHF 160.-

Plattformkosten: 171 CHF/Monat.

Hosting der Website: 142 CHF/Jahr *(gesponsert von: MJ MOTORSPORT)*

Marketing: Einmalig 100 CHF für die Einführungskampagne *(gesponsert von: MJ MOTOR-SPORT)*

3.5 Umsetzungsplan

Folgend wird der grobe umsetzungsplan aufgezeigt.

3.5.1 Phasen

Entwicklung (April): Erstellung der Kursmaterialien und Einrichtung auf Teachable.

Launch-Phase (Mai): Start der Marketingkampagne und Kursveröffentlichung.

Betriebsphase (Juni - Juli): Monitoring des Kurses, Sammeln von Feedback und Anpassungen.

Erweiterung: Einführung neuer Kurse jedes Quartal zur Erweiterung des Angebots.

Meilensteine: Kursfertigstellung bis Ende April, Erreichen von 50 Anmeldungen bis Ende Juni, Einführung neuer Kurse ab Oktober.

3.6 Risiken und Mitigation

Folgende Risiken müssen eingesehen werden:

Risiken:

a) Geringere als erwartete Anmeldezahlen.

b) Technische Probleme auf der Plattform Teachable.

Gegenmassnahmen:

➔ Frühzeitige Werbekampagnen und Nutzung von Social Media zur Steigerung der Sichtbarkeit.

➔ Regelmässige Überprüfung der Plattformperformance und schnelle Reaktion auf technische Herausforderungen. Folgen der Service-Plattform mit Alarming für Downzeiten von Teachable.

➔ Kurse „Grow your online Business“ & „How to sell Digital Downloads“ besuchen

3.7 Abschluss

CAT stärkt das Produktportfolio von MJ Cybersecurity Services und baut das Bewusstsein und die Kompetenz in Cybersecurity bei der Zielgruppe aus. Die regelmässige Einführung neuer Kurse und Digitale Downloads stärkt die Bindung und das Engagement der Teilnehmer.

4. Fact Sheet

Folgend sind die Daten für das CAT-Fact Sheet. Ein WhitePaper mit allen Informationen für den Kunden kann hier eingesehen werden:

DOWNLOADS | MJCS (mjcybersecurity.com)

4.1 Überblick und Beschreibung des Services

Der CAT-Service von MJ Cybersecurity Services bietet umfassende Online-Trainings zur Steigerung der Cybersecurity-Kompetenzen. Ziel ist es, sowohl Privatpersonen als auch Unternehmen durch realistische Szenarien und interaktive Inhalte im Umgang mit Cyber-Bedrohungen zu schulen. Dank Audios, Fallbeispielen, interaktive Quizzes und mehr sind CAT-Kurse Kurse die bleiben, für jeden Lerntypen!

4.2 Zielgruppe des Services:

Privatpersonen ohne IT-Hintergrund, die ihre persönlichen Daten besser schützen möchten.

Unternehmen, die bereits den Fake Phishing Mail Service nutzen oder an allgemeiner IT-Sicherheit interessiert sind.

4.3 Service-Eigenschaften

Verfügbarkeit: Der Service ist 24/7 erreichbar und somit bestens geeignet in jeden Zeitplan zu passen.

Die Servicezeiten hängen von Teachable.com ab. Diese haben dazu eine Service-Page welche man sich für ein Alarming bei Downzeiten einschreiben kann.

4.4 Service Level Agreements (SLAs):

99% Betriebszeitgarantie nach Teachable-Plattform

Antwortzeiten von maximal 24 Stunden auf alle Anfragen durch MJ Cybersecurity Mitarbeiter.

4.5 Sicherheitsmerkmale und Compliance-Informationen:

Alle Daten werden gemäss DSG behandelt, ein Mini-DSG pro Service besteht.

4.6 Technische Details

Folgend werden die Technischen Details des CAT-Serivces aufgelistet.

4.6.1 Plattformen und Technologien:

Der Service basiert auf der Online-Lernplattform Teachable, die es ermöglicht, interaktive Kurse einfach zugänglich zu machen.

Inhalte umfassen Videos, MiniGames, Audioaufnahmen und interaktive Fallstudien.

4.6.2 Integration mit anderen Services und Systemen:

Nahtlose Integration mit allen Browserfähigen Geräten.

4.7 Kosten und Preismodell

Die genaue Berechnung kann dem Kapitel ROI entnommen werden.

4.7.1 Kostenstruktur:

Für Unternehmen welche den FPM-Service kaufen, erhalten CAT umsonst dazu.

Für Privatpersonen stehen die Kurse ab CHF 25.- pro Kurs zur Verfügung.

4.7.2 Mögliche Rabatte oder Staffelpreise:

Einführungsangebote und Rabatte für Neukunden

Gratis Digitale Downloads

4.8 Support- und Kontaktinformationen

Folgend sind die Support & Kontaktinfirmationen zu finden. Alles ebenso auf den White-Papers.

4.8.1 Erreichbarkeit des Supports:

Der Support für die CAT-Plattform wird via MJCS geschehen, folgend sind die Support- & Reaktionszeiten.

Täglich von 08:00 bis 21.30 Uhr, ausser an Feiertagen.

Erstantwortzeit bei CAT: Max. 24h

Support verfügbar via E-Mail und Kontaktformular auf mjcybersecurity.com

4.9 Eskalationsprozeduren und wichtige Kontaktpersonen:

Direkter Kontakt zur Inhaberin J. Storrer für alle Anliegen.

4.10 Nutzungsstatistiken und Performance-Indikatoren

Statistiken zur aktuellen Nutzung und Performance-Berichte:

Quartalsmässige Berichte über Kursanmeldungen und Feedback-Statistiken.

Monitoring der Engagement-Raten und Feedbacks für Kurse

4.11 Zugriff und Berechtigungen

Zugriff wird nur MJCS haben auf die Admin- & Kursstruktur. Dort können Kurse, Sales, Benutzer/Teilnehmende verwaltet werden.

Geschützter Zugang mit eigenem Login zu Trainingsmaterialien für die Teilzunehmenden.

4.12 Implementierungs- und Migrationsdetails

4.12.1 Schritte zur Einführung des Services für neue Nutzer:

Einfache Onboarding-Prozesse, unterstützt durch detaillierte Anleitungen und persönliche Unterstützung bei Bedarf. Alles Zentral auf mjcybersecurity.com

4.12.2 Dokumentation und Schulungsressourcen

Umfassende Nutzerhandbücher und Anleitungen auf mjcybersecurity.com.

Quartalsweise aktualisierte Online-Workshops und Tutorials.

4.13 Geplante Erweiterungen oder Verbesserungen:

Quartalsweise neue Kurse und Aktualisierungen der Trainingsinhalte basierend auf dem neuesten Feedback der Kunden/Teilnehmenden und den neuesten Trends in der Cybersecurity.

Release-Zyklus und Wartungsfenster sind so geplant, dass sie minimale Unterbrechungen gewährleisten und stets die aktuellsten Sicherheitspraktiken bieten.

5. Testcases / Testprotokolle

Für das Testen wurde eine Person ausgewählt, welche die Usersicht testet. Die Admin-Sichten wurden von jst getestet. Beide Tests werden in einem Testprotokoll protokolliert.

Die Testprotokolle sind im folgenden Dokument einzusehen:

ID2132_StorrerJessica_CAT_Testprotokoll_v1.pdf

6. Ausführung

In diesem Abschnitt wird der Aufbau der Website mjcybersecurity.com und der Aufbau der Kurse und Website von mjcybersecurity.teachable.com erläutert.

6.1 MJCS – mjcyberseucrity.com

Als erster Berührungspunkt für Kunden wird eine Website erstellt. Diese dient rein zur Übersicht, was MJCS anbietet.

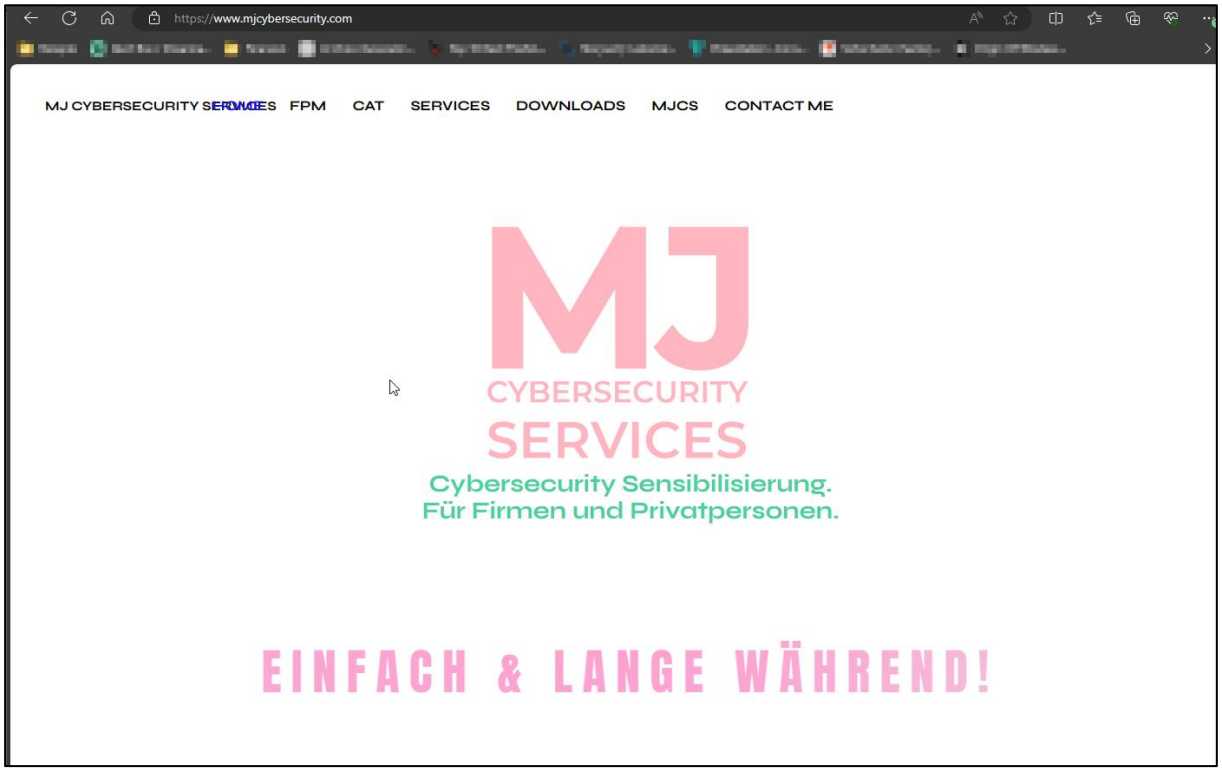


Abbildung 1 - Home mjcybersecurity.com

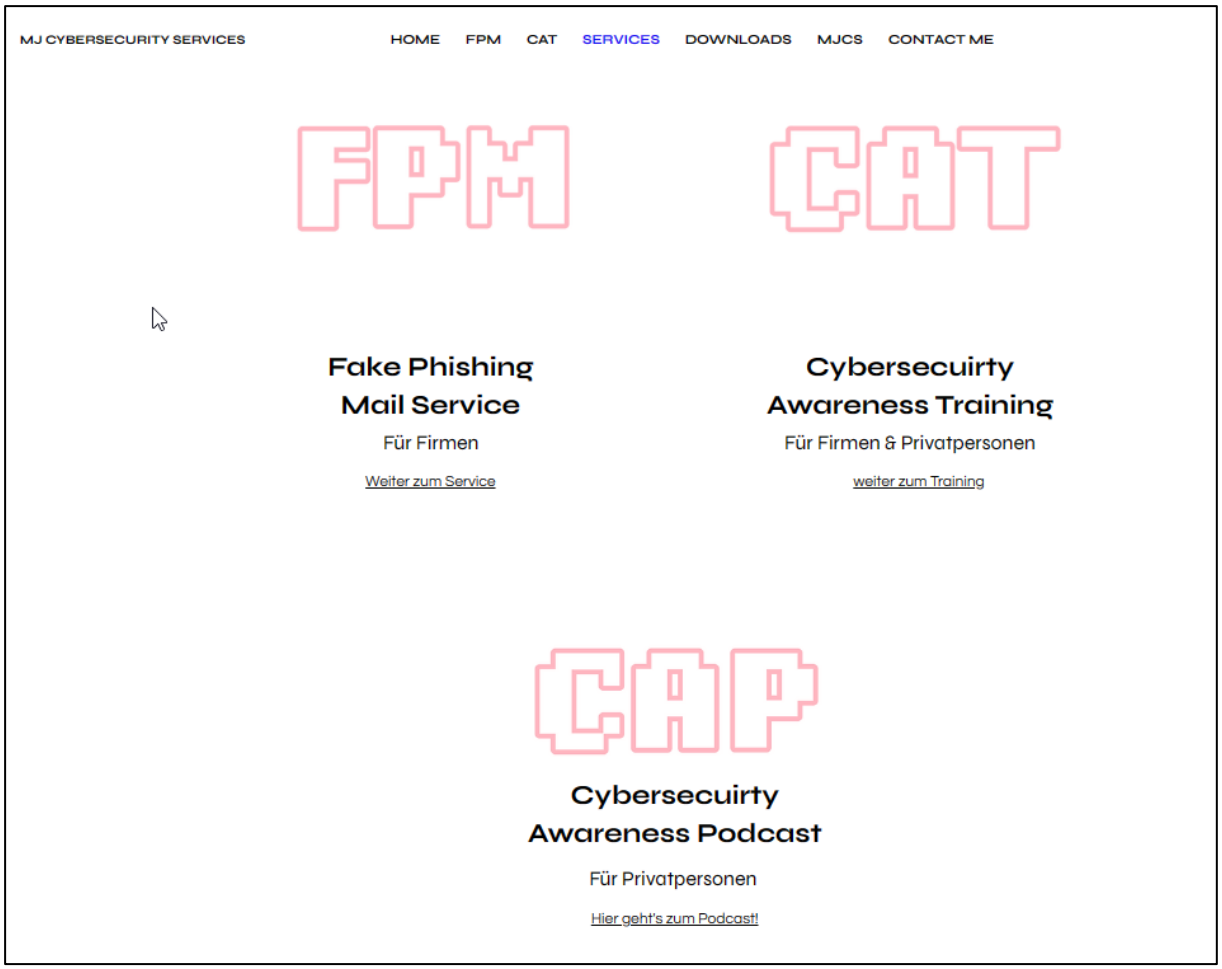


Abbildung 2 - Anpreisung Services auf mjcybersecurtiy.com

Abbildung 3 - weitere Anpreisung des Services

6.1.1 Startseite (Homepage)

Übersicht: Die Startseite legt den Fokus auf Sensibilisierung und Bildung im Bereich Cybersecurity, maßgeschneidert für Unternehmen und Privatpersonen. Der Slogan „einfach & lange während!“ spiegelt das Ziel wider, klare und nachhaltige Schulungen anzubieten.

Services:

Fake Phishing Mail Service: Zielt darauf ab, Unternehmen dabei zu unterstützen, Mitarbeiter im Erkennen von Phishing-Versuchen zu schulen.

Cybersecurity Awareness Training: Für Unternehmen und Privatpersonen über eine spezialisierte Plattform verfügbar.

Cybersecurity Awareness Podcast: Behandelt Cybersecurity-Themen in verständlicher Weise.

Newsletter: Ermutigt Besucher, sich für Cybersecurity-Tipps und Berichte zur Klickrate anzumelden.

Call-to-Actions:

Link zur Trainingsplattform

Link zum Podcast

Werbung für:

Fake Phishing Mail Service

Cybersecurity Awareness Training

Cybersecurity Awareness Podcast (MJCS)

Kurse

Übersicht: Verschiedene Kurse zum Thema Cybersecurity Awareness Training.

Wichtige Kurse:

Fake Phishing Mails (FPM): Konzentriert sich auf das Erkennen von Phishing-Mails durch Simulationen.

Cybersecurity Awareness Training (CAT): Ein allgemeines Schulungsprogramm für Cybersecurity.

Call-to-Actions:

„Mehr erfahren“-Links zu detaillierten Kursinformationen

Direkte Links zur Trainingsplattform (MJCS)

Newsletter-Anmeldung: Ermutigt die Nutzer, sich für weitere Cybersecurity-Tipps anzumelden.

Call-to-Action:

Direkter Link zur Trainingsplattform (CAT)

6.1.2 Weitere Bereiche

FPM

Erklärung des Services inkl. Beispielreport

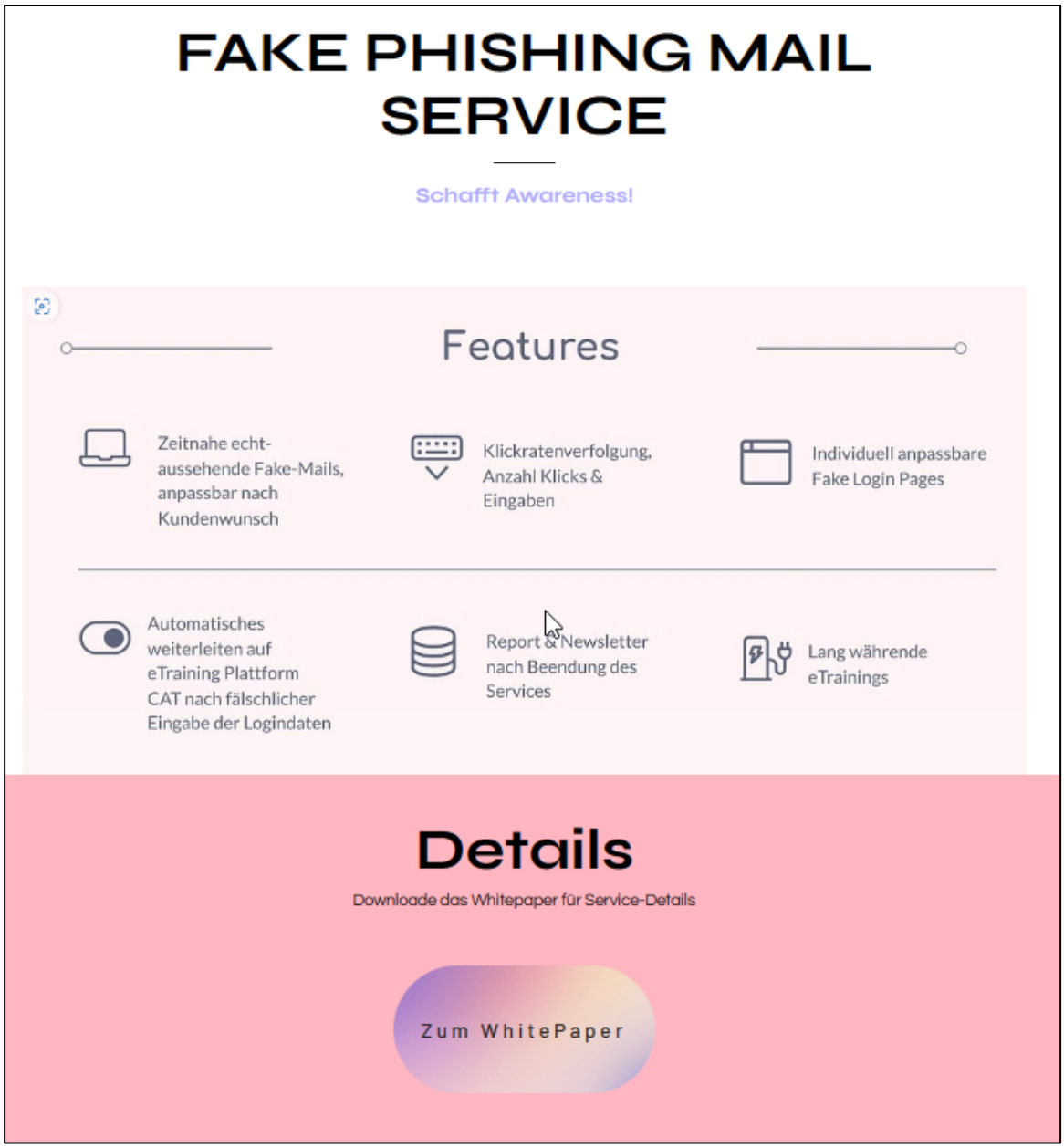


Abbildung 4 - FPM-Site von mjcybersecurity.com

Abbildung 5 - Weitere FPM-Service Details

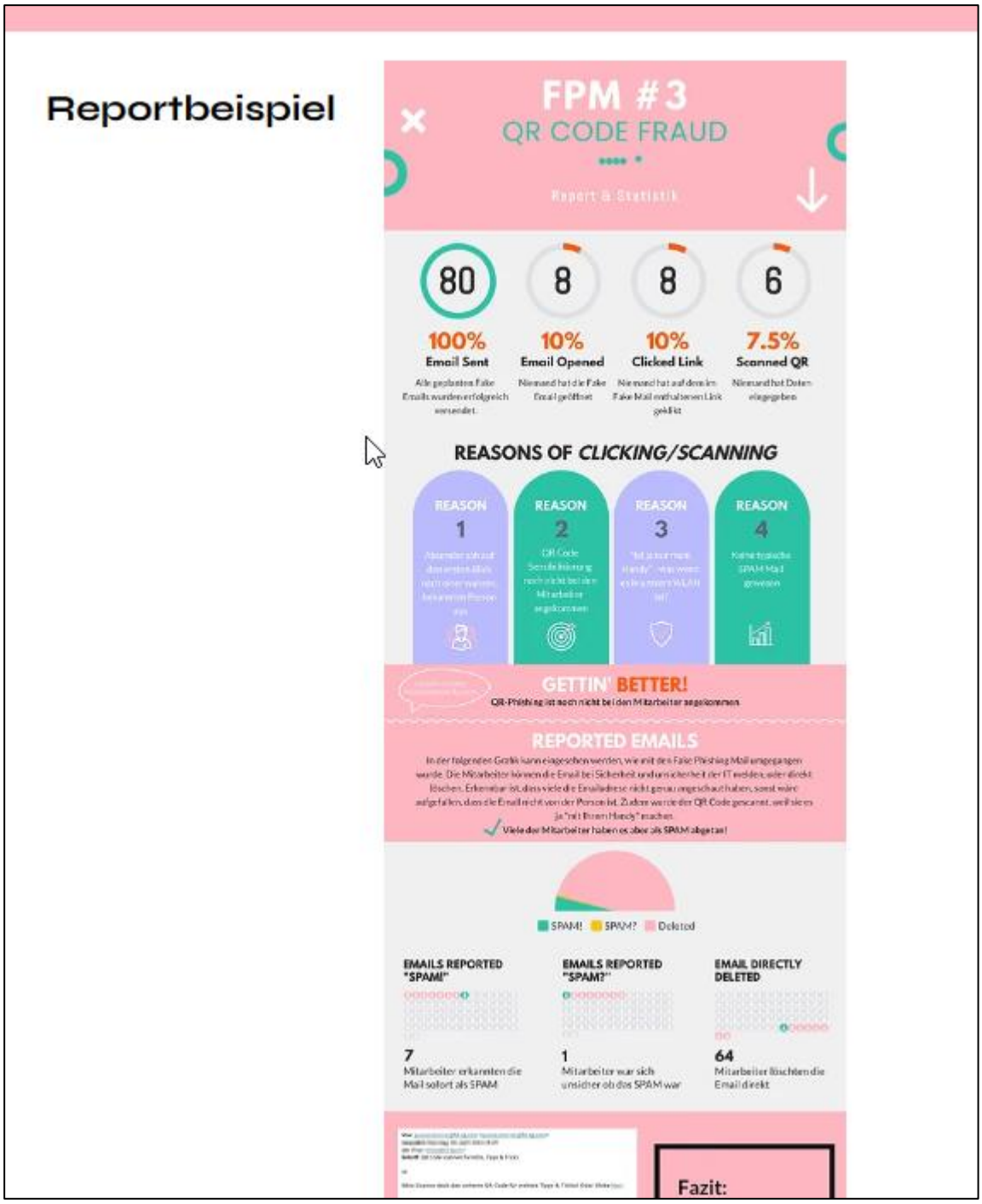


Abbildung 6 - FPM-Reportbeispiel für Kunden

CAT

How To für CAT Plattform und Anmeldung

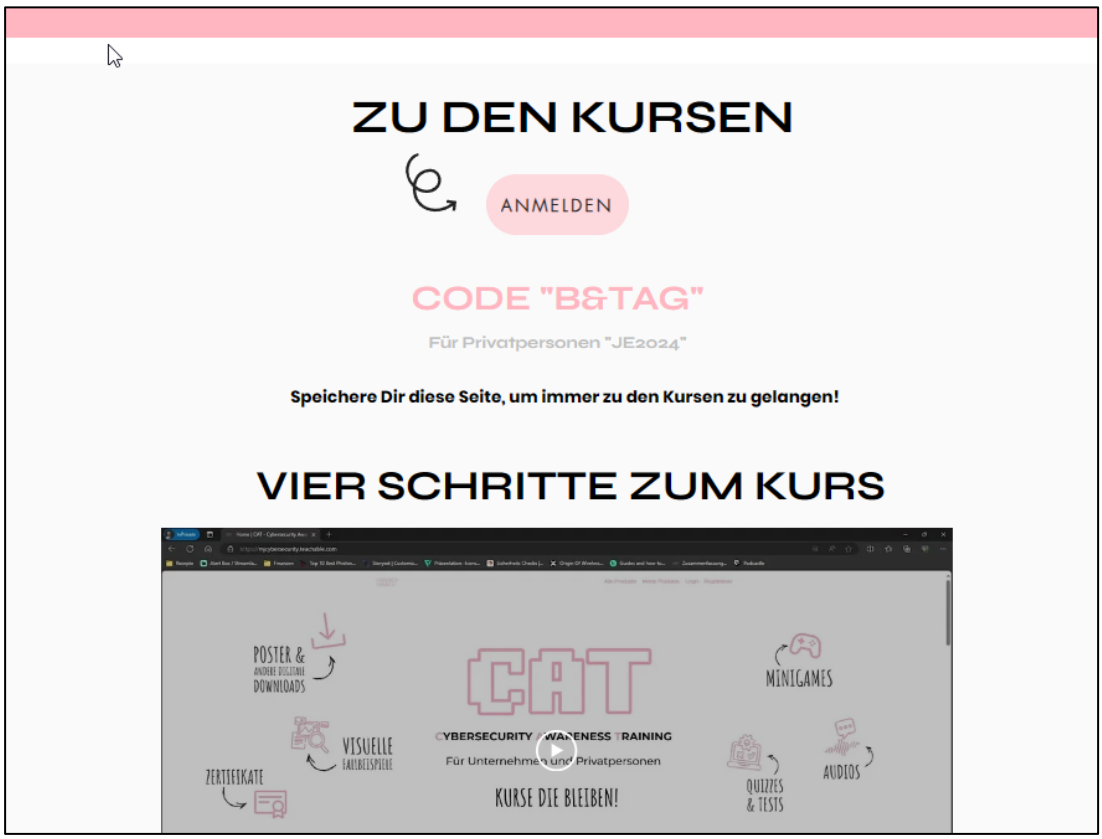


Abbildung 7 - How To CAT

Downloads

WhitePapers zu den Services und Kundenonboarding.

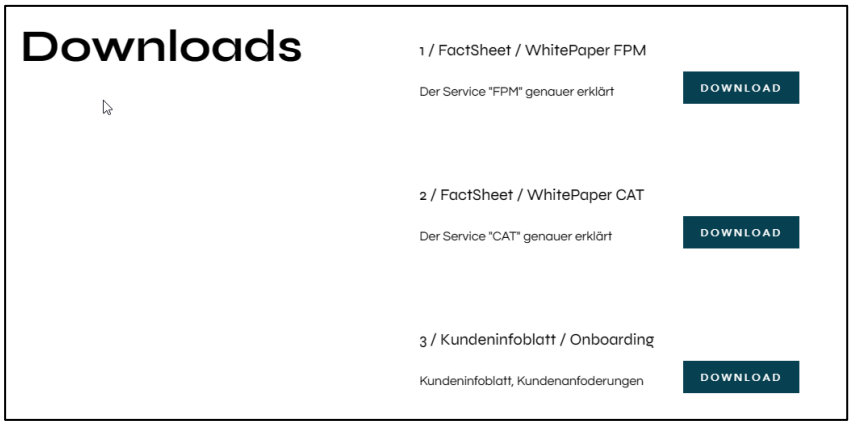


Abbildung 8 - WhitePaper/FactSheet/KundenonboardingBeispiel Download pro Service

QR-Phishing

Als „Guerilla“ Werbung wurde eine QR-Phishing Page eingerichtet

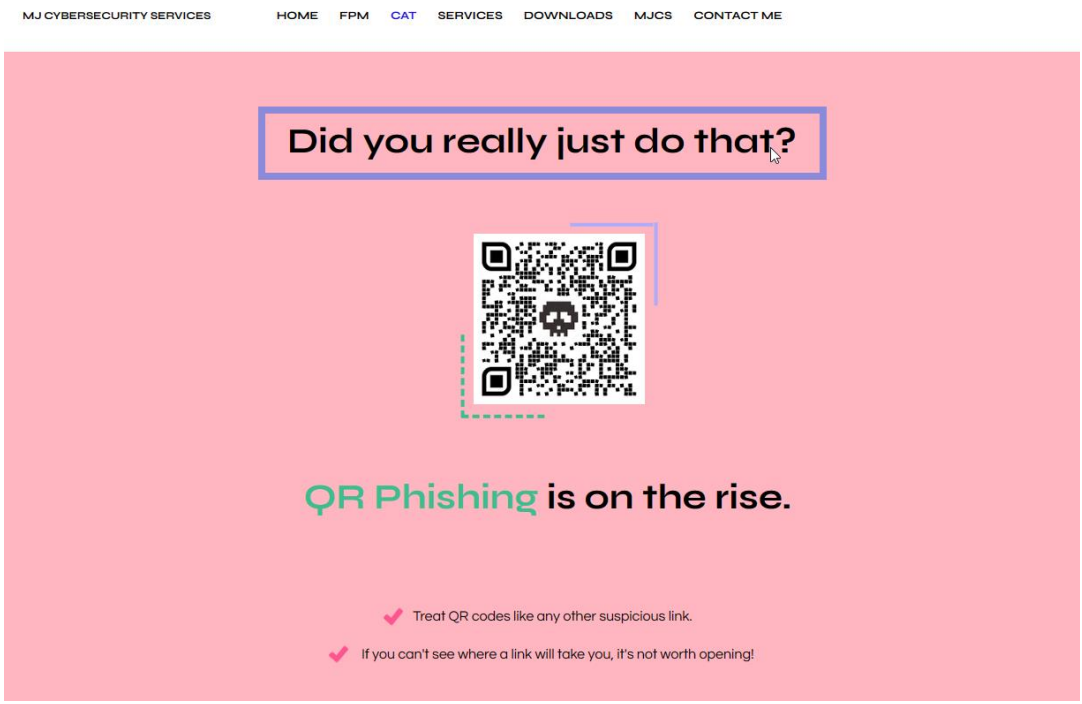


Abbildung 9 - QR-Phishing

Oopsie-Page

Diverse Oopsie-Pages für die FPM-Kunden, welche bei fälschlicher eingabe der Logindaten auf der Fake Login Page auf diese Seite redirected werden.

Abbildung 10 - Oopsie Page B&T AG

MJCS (Über Uns):

Informationen über das Unternehmen und ihren Ansatz zu Cybersecurity.

Abbildung 11 - Über uns

Kontakt

Ein Kontaktformular für Anfragen.

Footer

mit Newsletter und wichtigen Links

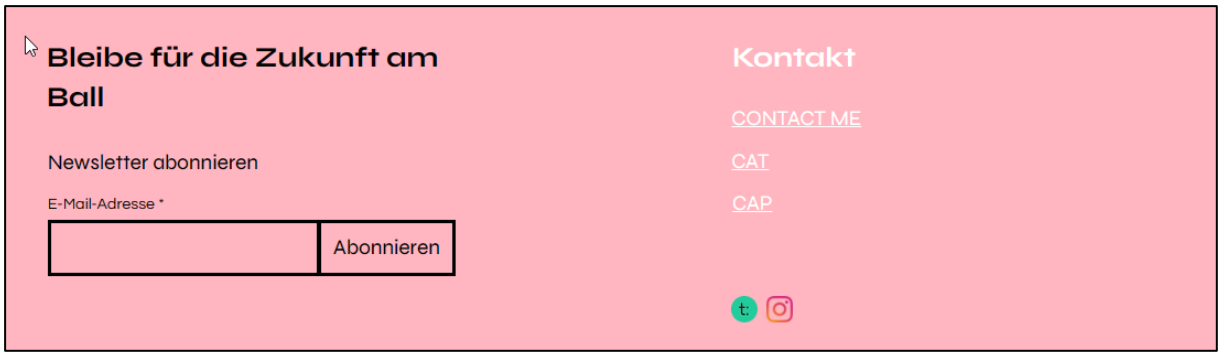


Abbildung 12 - Footer

Rechtliche Informationen:

AGB

Cookie-Richtlinie

Datenschutzrichtlinie

Impressum

6.2 CAT – mjcybersecurity.teachable.com

Die Plattform mjcybersecurity.teachable.com bietet strukturiertes Cybersecurity Awareness Training mit dem Hauptfokus auf Phishing-Mails. Die Kurse sind einsteigerfreundlich und angereichert mit praktischen Übungen, Quizfragen und realen Beispielen. Zudem haben die Teilnehmenden mit sogenannten „Antwortkasten“ platz Ihr Feedback dazulassen.

Übersicht der Plattform / Start

Zweck: Bietet umfassendes Cybersecurity Awareness Training mit dem Schwerpunkt auf der Erkennung von Phishing-Mails und dem Verständnis von Online-Bedrohungen.

Zielgruppe: Abgestimmt auf Unternehmensmitarbeiter und Einzelpersonen, die sich für grundlegende Cybersecurity-Themen interessieren.

Kursstruktur: Woche 1-3 & Digitale Downloads

Erzählung über MJCS und Kursleiter/in (Je/Jessica)

Fokus auf die Vereinfachung von Cybersecurity-Konzepten für ein breites Publikum.

Bietet praxisnahe und ansprechende Schulungen sowohl für Unternehmen als auch für den persönlichen Gebrauch (Home).

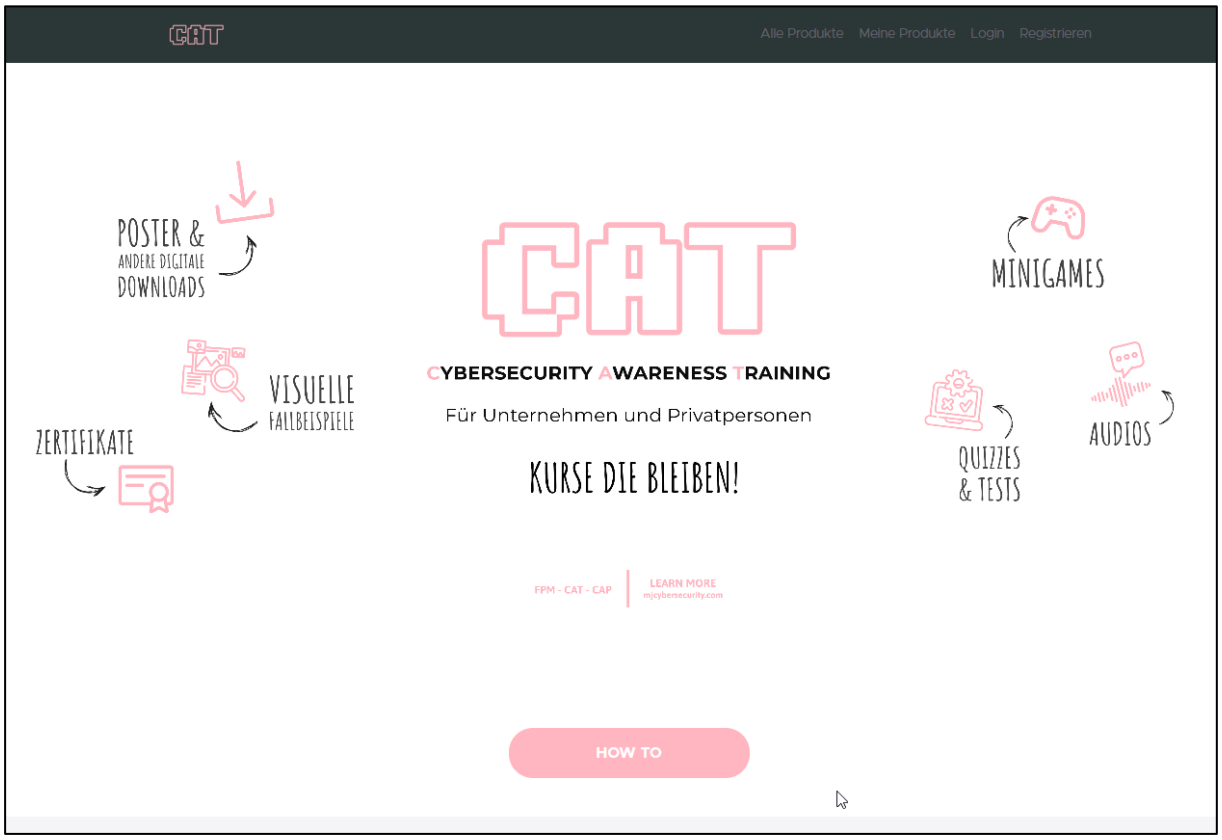


Abbildung 13 - Einstiegsseite CAT auf Teach:able

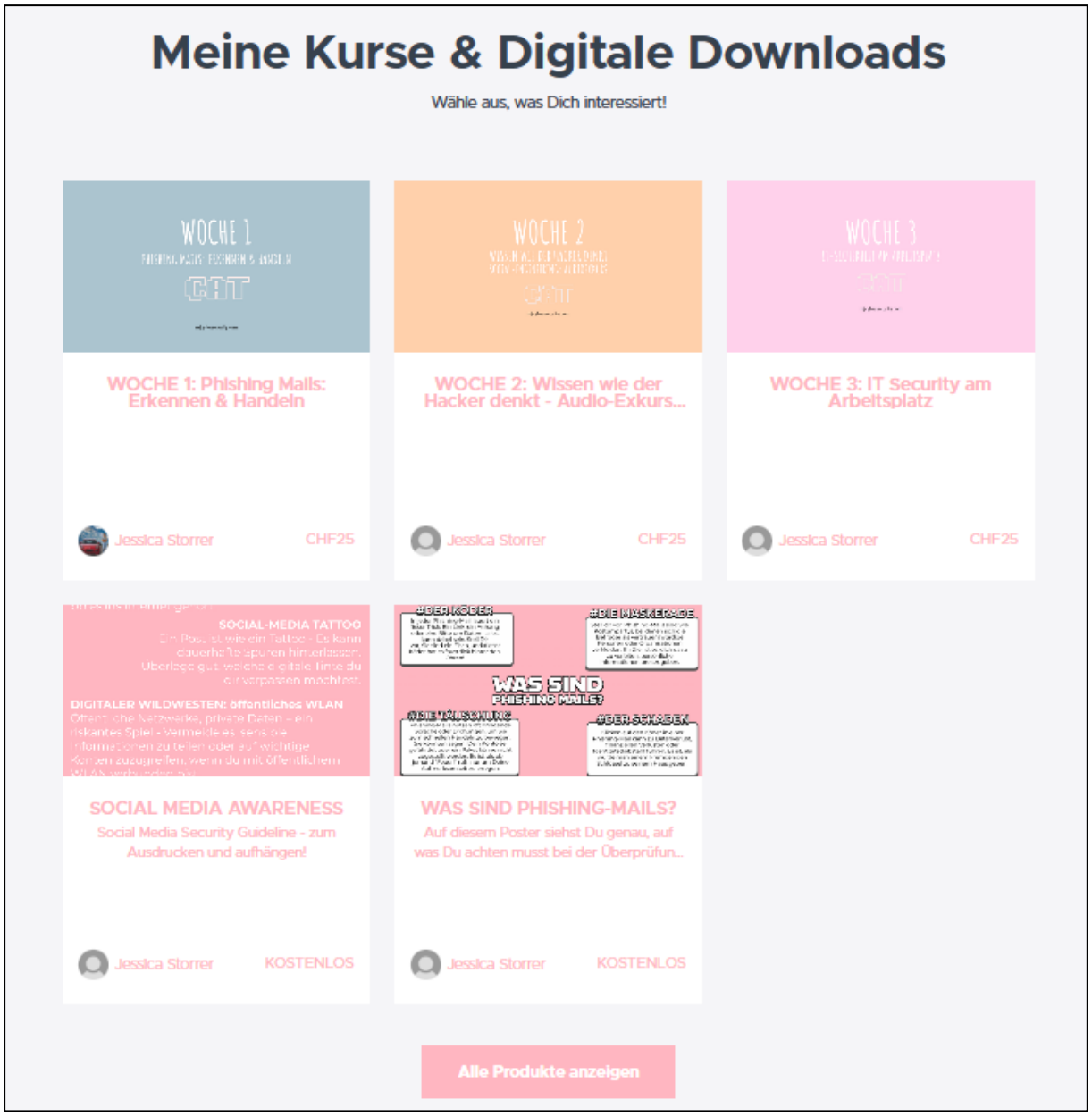


Abbildung 14 - Angebotene Kurse auf Einstiegsseite

6.3 Woche 1: Phishing Mail: Erkennen & Handeln

Der Kurs ist über eine Woche strukturiert und in fünf Tage mit jeweils unterschiedlichen Inhalten aufgeteilt:

6.3.1 TAG 1 (Tag 1): Einführung & Einführung in Phishing-Mails

Inhalt:

Einführung in Phishing-Mails und ihre Arten.

Überblick über bekannte Phishing-Hacks.

Aktivitäten:

Praktische Übungen zum Verständnis der Grundlagen von Phishing.

Lektionen:

- Wie dieser Kurs funktioniert
- Was sind Phishing-Mails?
- Die verschiedenen Arten von Phishing-Mails
- Die bekanntesten Phishing-Mail-Hacks
- Zusammenfassung TAG 1 (Home).

6.3.2 TAG 2 (Tag 2): Phishing-Mails erkennen

Inhalt:

Erkennen von Phishing-Mails und verdächtigen Anhängen.

Aktivitäten:

Übung „Finde die Phishing-Mail“.

Test zur Identifizierung von Phishing-Mails.

Lektionen:

- Erkennen verdächtiger Links und Anhänge
- Finde die Phishing-Mail
- Zusammenfassung TAG 2

Test: Phishing-Mail erkennen (Home).

6.3.3 TAG 3 (Tag 3): Fallstudien und Praxisbeispiele

Inhalt:

- Fallstudien und praktische Beispiele von Phishing.
- Der gefälschte Kundendienst - Phishing per Telefon
- Phishing via WhatsApp, SMS und andere Plattformen.

- Zusammenfassung TAG 3 (Home).

6.3.4 TAG 4 (Tag 4): Melden und Handeln bei Phishing-Mails

Inhalt:

Best Practices für das Melden von Phishing-Mails und angemessene Reaktionen.

Lektionen:

- Richtiger Umgang mit Phishing-Mails
- Report an IT
- Zusammenfassung TAG 4

6.3.5 TAG 5 (Tag 5): Zusammenfassung des Kurses

Zusammenfassung:

Rückblick auf die Lektionen der Woche.

Abschließendes Quiz zur Bewertung des Wissens der Teilnehmer.

Dankesnachricht und Tipps, um auf dem neuesten Stand zu bleiben (Home).

Wichtige Merkmale des Kurses

- Abschluss-Quiz: Ein interaktives Quiz am Ende zur Überprüfung des Wissens der Teilnehmer.

Fazit

Der Kurs „Phishing-Mails: Erkennen & Handeln“ ist umfassend und legt den Fokus auf praktische Übungen, Fallstudien und Abschlussprüfungen, um den Teilnehmern zu helfen, Phishing-Bedrohungen zu erkennen und darauf zu reagieren. Der Kurs richtet sich an ein breites Publikum und stellt sicher, dass sowohl Unternehmensmitarbeiter als auch Einzelpersonen vom Training profitieren können. Die Audios und Fallbeispiele runden die Kurse ab.

6.3.6 Eindrücke vom Kurs Woche 1 – Phishing Mails: Erkennen & Handeln

Folgend werden in Bilder die Eindrücke des Kurses wiedergegeben.

Eindrücke	Beschriftung Bild
	**Abbildung 15 - Einstiegsseite Kurs Woche 1**

Abbildung 16 - Übersicht Kursplan Woche 1

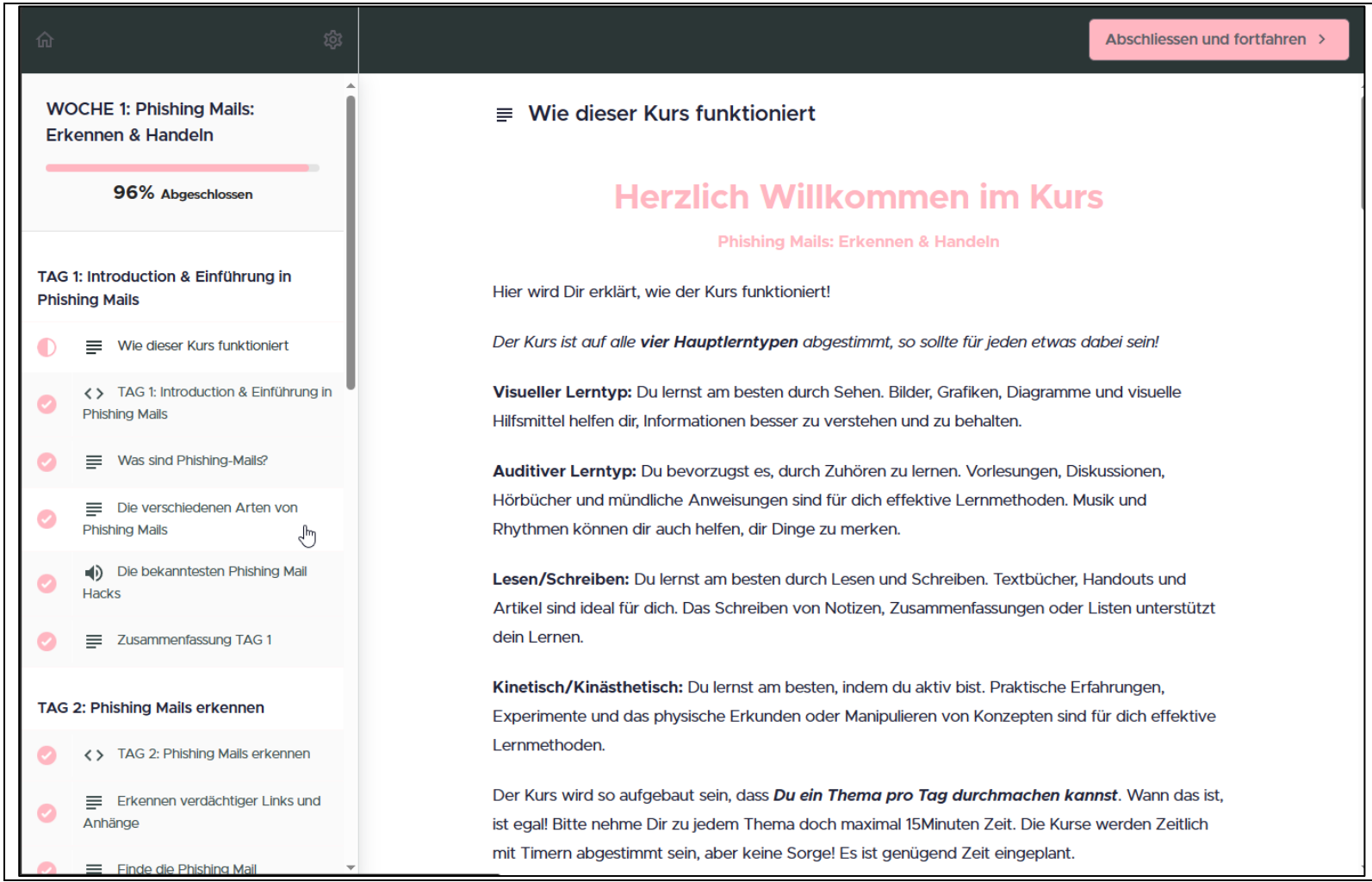


Abbildung 17 - Übersicht Kurs

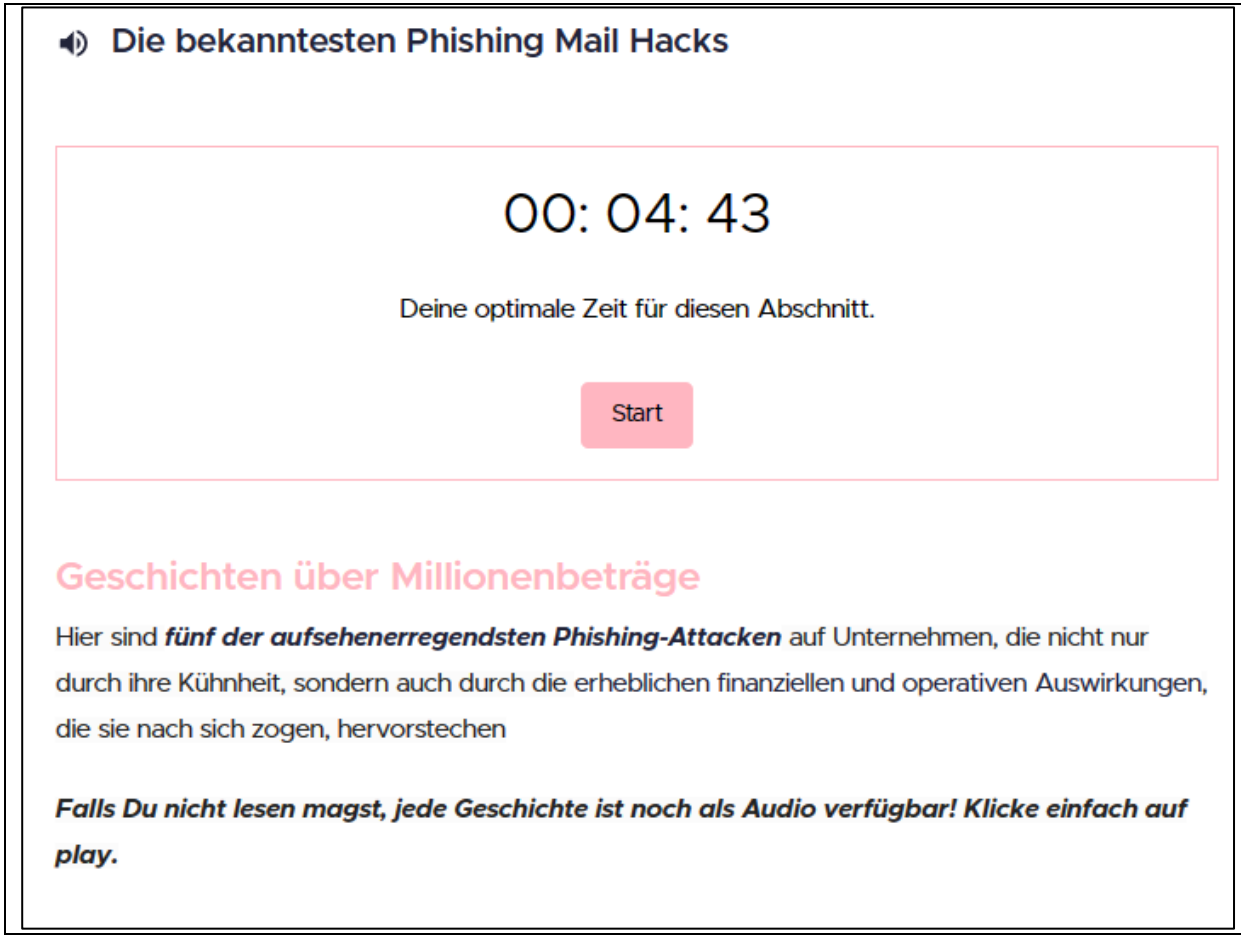


Abbildung 18 - Mit Timer versehen

Der große Coup bei FACC

Stell dir vor, du bist bei einem österreichischen Luftfahrtzulieferer angestellt und bekommst eines Tages eine E-Mail, die scheinbar vom CEO kommt. Die Nachricht bittet dich, €42 Millionen für ein angebliches Akquisitionsprojekt zu überweisen. Ohne den Betrug zu erkennen, folgst du der Anweisung – nur um später festzustellen, dass du einem der kühnsten Phishing-Angriffe zum Opfer gefallen bist. Die Konsequenzen sind dramatisch: hochrangige Führungskräfte, inklusive des CEO, verlieren ihren Job, und es entbrennt ein Rechtsstreit um Schadensersatzforderungen, die jedoch abgewiesen werden (IT Governance).

Drücke hier auf Play....

▶ der grossce coiup bei facc.mp3

Abbildung 19 - Geschichten auch als Audio Verfügbar

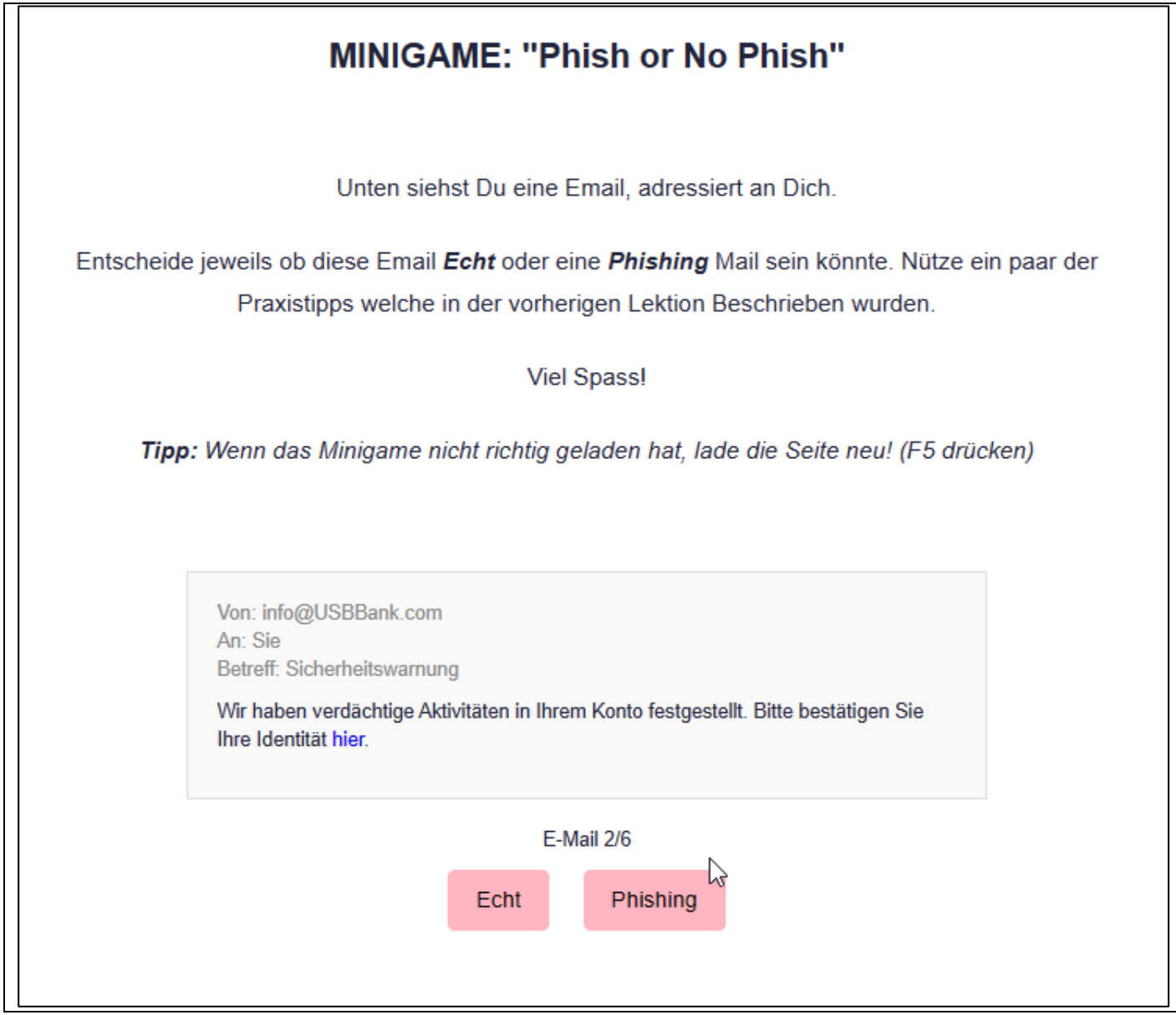


Abbildung 20 - Diverse Mini-Games

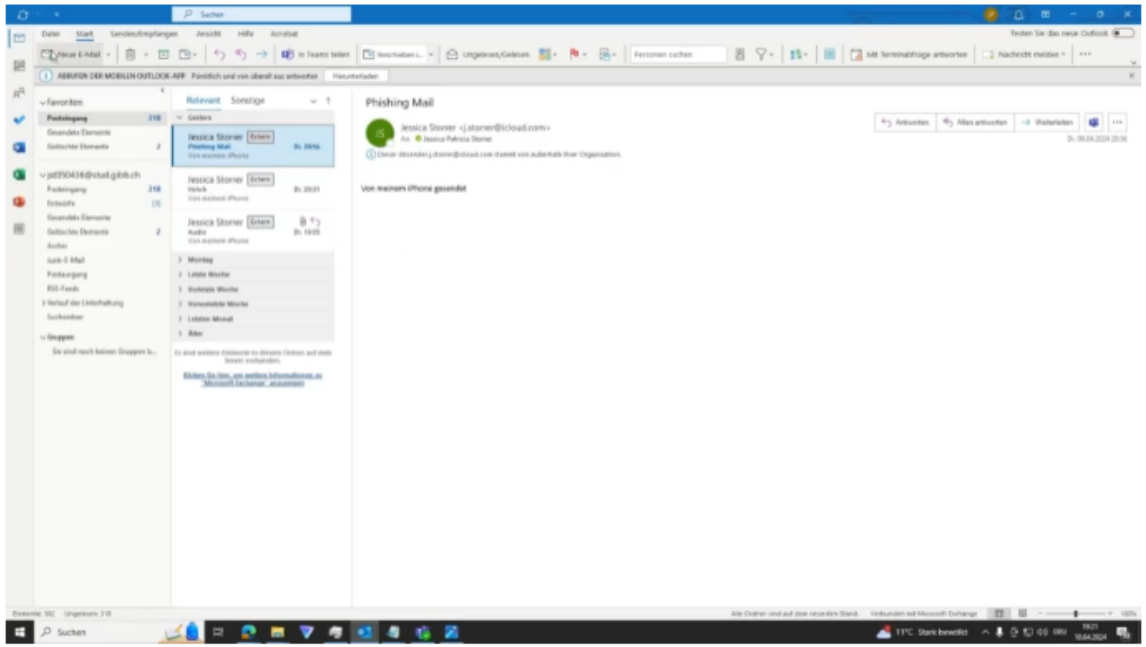
Doch wie leite ich die Email korrekt weiter, ohne sie öffnen zu müssen? Siehe im nächsten Video wie Du das vermeintliche Email korrekt weiterleitest und an die IT Reportest. 		**Abbildung 21 - "How-To" Videos**

Abbildung 22 - Interaktives Lernen

Überprüfe die URL genau

Erkennungsmerkmale: Die URL enthält ungewöhnliche oder falsch geschriebene Wörter, die auf den ersten Blick leicht zu übersehen sind.

Beispiel: Ein Link, der zu „www.amaz0n.com“ statt „www.amazon.com“ führt.

PRAXISTIPP: ***Fahre mit der Maus über den Link - dann wird er Dir angezeigt! (nicht klicken, nur drüberfahren)***

Verwendung von URL-Verkürzen

Erkennungsmerkmale: Der Link ist mit einem URL-Verkürzungsdienst wie bit.ly oder TinyURL erstellt worden, was die wahre Bestimmung des Links verschleiert.

Beispiel: Ein Link, der aussieht wie „bit.ly/12345“, ohne Hinweise auf das Ziel.

PRAXISTIPP: ***Fahre mit der Maus über den Link - dann wird er Dir angezeigt! (nicht klicken, nur drüberfahren)***

Ungewöhnliche Dateianhänge

Erkennungsmerkmale: Anhänge mit unerwarteten Dateiendungen, besonders solche, die ausführbare Dateien kennzeichnen (z.B. .exe, .scr, .zip).

Beispiel: Eine E-Mail, die behauptet, eine Rechnung zu enthalten, aber mit einer .exe-Datei ankommt.

PRAXISTIPP: ***Bei Unsicherheit -> Email an IT weiterleiten***

Ungewohnte Aufforderungen zum Download oder Öffnen

Abbildung 23 - Div. Praxistipps direkt zum Umsetzen

"Hörenverstehen" Phishing per Telefon

Nachfolgend hörst Du drei Konversationen. Alle drei Konversationen handeln sich in Firmen ab, wo die Empfangsarbeitende Person alle eigehenden Telefonate einer Firma abnimmt und bearbeitet.

Es ist nun rauszufinden, ob die Anrufende Person auf Phishing aus ist UND welche Unternehmensinformationen man preisgeben darf, und welche nicht.

Höre gut zu und beantworte im Anschluss die Fragen!

(Du kannst die Audios immer wieder von vorne anhören, beachte aber dabei die Zeit!)

Fallbeispiel Nummer 1

Drücke hier auf Play

▶ Fallbeispiel Nr. 1.MP3 (1).mp3

Fallbeispiel Nummer 2

Drücke hier auf Play

Abbildung 24 - Hörenverstehen Fallbeispiele

Abbildung 25 - Aktuell bleiben

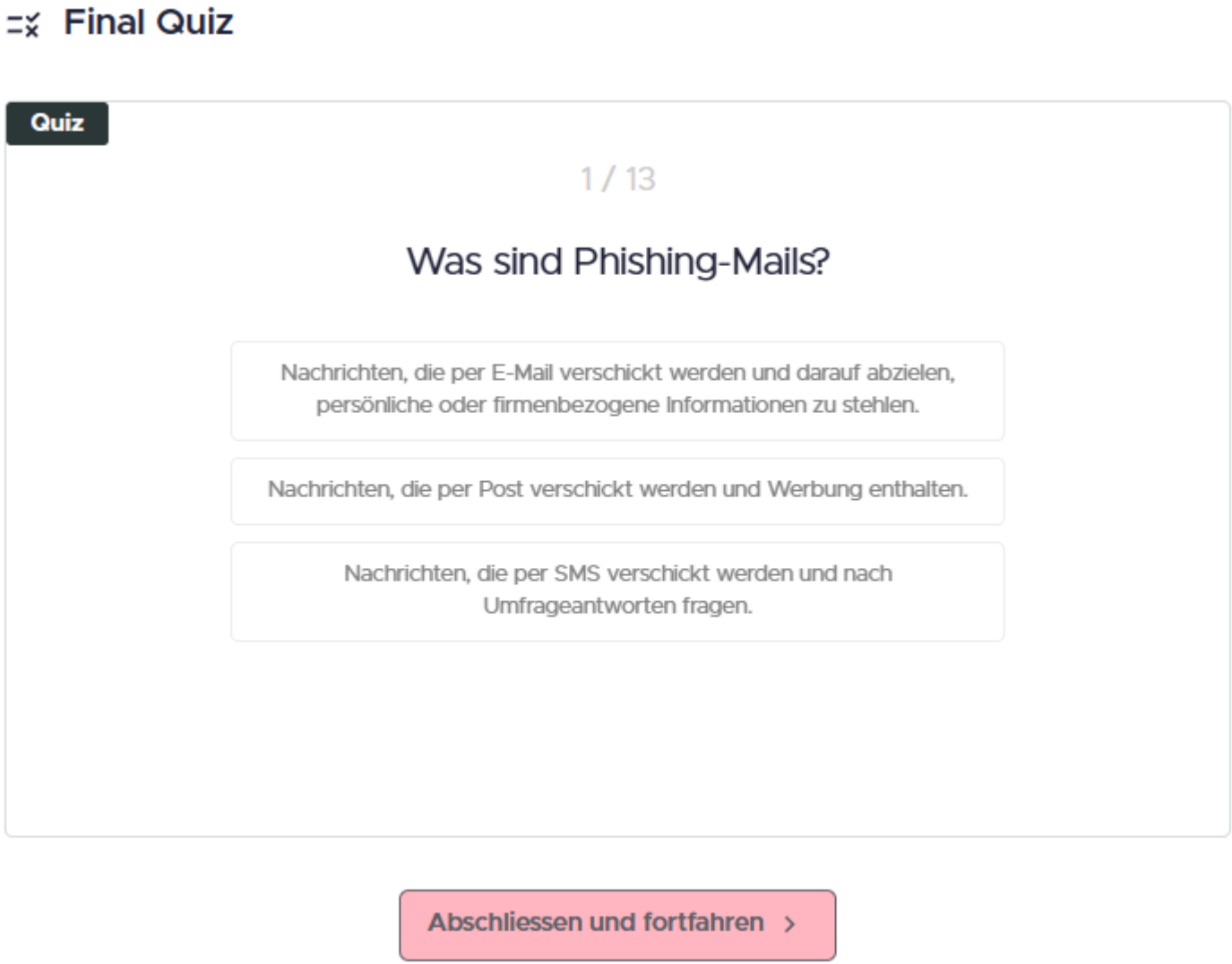


Abbildung 26 - Quizzes

	**Abbildung 27 - Antwortkasten für Feedback**

Tabelle 1 - Eindrücke Kurs "Woche 1 Phishing Mails: Erkennen & Handeln"

6.4 Woche 2: Wissen wie der Hacker denkt: Audioexkurs zu Social Engineering

In diesem Kurs werden vier Audio-Gescichten bezüglich den vier Haupttechnicken von Socia-lEngineering erzählt. Alles sollten persönliche Geschichten sein, denn diese halten sich besser im Hirn.

6.4.1 TAG 1 Social Engineering: Vertrauen und Autorität

- Einführung / Wie der Kurs funktioniert
- Social Engineering Tag 1: Vertrauen und Autorität
- Zusammenfassung TAG 1

6.4.2 TAG 2 Social Engineering: FOMO & Dringlichkeit & Knappheit

- Social Enigneering Tag 2: FOMO & Dringlichkeit & Knappheit
- Zusammenfassung Tag 2

6.4.3 TAG 3 Social Engineering: Gegenseitigkeit & Norm der Gegenseitigkeit (Reziprozität)

- Social Enigneering Tag 3: Gegenseitigkeit & Norm der Gegenseitigkeit
- Zusammenfassung Tag 3

6.4.4 TAG 4 Social Engineering: Emotionale Manipulation

- Social Enigneering Tag 4: Emotionale Manipulation

6.4.5 Zusatz - TAG 5: Achtsamkeit

- Achtsam durch den Alltag - Warum?
- Atemübung für Überall

6.4.6 Einblicke Woche 2 Wissen wie der Hacker denkt: Audioexkurs zu Social Engineering

Folgend werden bildlich die Eindrücke der zweiten Woche – dem reinen Audioexkurs – gezeigt.

Abbildung 28 - Übersicht Kurs Woche 2

Herzlich Willkommen im Kurs

Wissen wie der Hacker denkt - Audio-Exkurs Social Engineering

Kopfhörer raus! Wir hören uns Geschichten an!

Diese Woche Kurs beinhaltet nur vier Tage *(+1 Zusatztag wer mag)*, an jedem Tag bekommst Du ein ***Hörspiel*** einer kurzen - wahren - ***Geschichte über die vier wichtigsten Social Engineering Praktiken!***

Warum Geschichten? So bleiben die wichtigsten Punkte des Themas einfacher in Erinnerung!

Keine Sorge wenn Du grad keine Kopfhörer dabei hast. Die Audios sind Downloadbar und Du kannst Dir das Audio somit einfach "nach Hause schicken" oder auf Deinem Smartphone hören. (Schick Dir einfach eine Email mit dem Audiofile, aber bitte sende die nicht herum!)

Abschliessen und fortfahren ›

Abbildung 29 - Wie der Kurs funktioniert

Social Engineering TAG 1: Vertrauen und Autorität

Social Engineering ist eine ***Methode der Informationsbeschaffung***, bei der ***psychologische Manipulation*** genutzt wird, um Personen dazu zu bringen, ***vertrauliche Informationen preiszugeben oder bestimmte Aktionen auszuführen***. Das Ziel ist es oft, u***nberechtigten Zugang zu Systemen, Daten oder physischen Standorten*** zu erlangen.

Täter setzen dabei auf die ***Ausnutzung menschlicher Eigenschaften wie Vertrauen, Autoritätsgläubigkeit und Hilfsbereitschaft***. Sie täuschen Identitäten vor, erschaffen gefälschte Szenarien oder nutzen Dringlichkeit und Angst, um ihre Opfer zu manipulieren.

Da dieser Ansatz die menschliche Psyche statt technische Schwachstellen ausnutzt, kann er besonders schwer zu erkennen und zu verhindern sein.

GESCHICHTE #1

Schauen wir uns mal an, wie Cyberkriminelle Social Engineering nutzen könnten, um Vertrauen und Autorität vorzutäuschen – und wie du dich davor schützen kannst.

Drücke hier auf Play....

▶ TAG1_SocialEngineering_Vertrauen&Autorität.mp3

Download

Abbildung 30 - Geschichte #1 Woche 2

Social Engineering TAG 2: FOMO & Urgency

In der Welt des Phishings sind FOMO und das Schaffen eines Gefühls von Dringlichkeit bewährte Tricks von Cyberbetrügern. Sie spielen mit unserer Angst, etwas zu verpassen oder zu spät zu kommen, um uns zu vorschnellen Handlungen zu verleiten.

GESCHICHTE #2

Schauen wir uns mal an, wie Cyberkriminelle Social Engineering nutzen könnten, um Urgency & FOMO hervorzulocken – und wie du dich davor schützen kannst.

Drücke hier auf Play....

▶ Social Engineering Tag 2 - FOMO.mp3

Download

Keine Kopfhörer zur Hand? Keine Zeit?

Kein Problem!

Lade Dir das File Runter! Aber schicke es niemandem Fremden!

Den kannst Du dir per Mail "heimschicken" und gemütlich mal auf Deinem Handy oder Zuhause nachhören!

Abbildung 31 - Geschichte #2 FOMO Woche 2

Social Engineering TAG 3: Norm der Gegenseitigkeit

Reziprozität ist ein sozialpsychologisches Prinzip, das auf Gegenseitigkeit beruht: Wenn jemand etwas für dich tut, fühlst du dich verpflichtet, den Gefallen zu erwidern. Cyberkriminelle nutzen genau diese Tendenz aus, um ihre Opfer auszutricksen. Ein klassisches Beispiel sind Phishing-Mails, die vorgeben, dir einen kostenlosen Ratgeber oder ein Geschenk zu bieten. Der Haken? Um das "Geschenk" zu erhalten, sollst du zuerst "nur schnell" ein Formular ausfüllen oder eine Umfrage beantworten.

GESCHICHTE #3

Schauen wir uns mal an, wie Cyberkriminelle Social Engineering nutzen könnten, um die Norm der Gegenseitigkeit hervorzulocken – und wie du dich davor schützen kannst.

Drücke hier auf Play....

▶ social engineering tag 3 Reziprozität.mp3

Download

Keine Kopfhörer zur Hand? Keine Zeit?

Kein Problem!

Lade Dir das File Runter! Aber schicke es niemandem Fremden!

Abbildung 32 - Geschichte #3 Reziprozität Woche 2

Social Engineering TAG 4: Emotionale Manipulation

In dieser Geschichte wird dir gezeigt, wie einfach du ein Auto öffnen lassen könntest. Diese zeigt dir dabei auch auf, auf welche Infos von dir du besonders acht geben musst.

Denn Telefonnummer werden schnell gespooft!

Du fragst Dich jetzt was spoofing ist und wie das gehen soll? Dann höre Dir die Geschichte bis zum Ende an!

In dieser Geschichte habe ich ein Selbstversuch gewagt zu Schulungszwecken. Ich habe mir überlegt, ob ich durch Anrufen des Supports einer grösseren Autofirma ein Auto öffnen lassen kann. Ob und wie dies geklappt hat, erfährst Du wenn Du Dir die Geschichte bis zum Ende anhörst!

Jegliches Hacken, Social Engineering etc. hat rechtliche Folgen und ist illegal!

GESCHICHTE #4

Schauen wir uns mal an, wie Cyberkriminelle Social Engineering nutzen könnten, um Dich emotional zu manipulieren – und wie du dich davor schützen kannst.

Drücke hier auf Play....

▶ Social Engineering Tag 4.MP3 (original).mp3

Abbildung 33 - Geschichte #4 Auto öffnen lassen Woche 2

Atemübung für Überall

Diese kurze Achtsamkeitspause ist dafür gedacht, euch 2 Minuten der Entspannung und fokussierten Ruhe zu bieten. Nehmt euch diese Zeit, wenn Ihr wollt.

Diese Übung kannst Du ganz einfach in Deinen Alltag einbauen, sei es auf dem WC, während ihr auf das Aufwärmen eures Mittagessens an der Mikrowelle wartet, oder auch einfach zwischendurch, wenn ihr ein paar Minuten zu atmen und zu entspannen braucht.

Atemübung **(2 Minuten)**:

1. Setzt euch auf einen bequemen Stuhl oder bleibt stehen, je nachdem, wo ihr euch befindet.
2. Atmet langsam und tief ein. Zählt dabei leise bis vier.
3. Haltet den Atem für zwei Sekunden.
4. Atmet langsam aus, während ihr wieder bis vier zählt.
5. Wiederholt diese Atemübungen für drei Minuten. Konzentriert euch voll und ganz auf euren Atem und darauf, wie die Luft eure Lungen füllt und verlässt.

Diese einfache Übung könnt ihr wirklich überall durchführen. Sie hilft nicht nur, Stress abzubauen, sondern ***verbessert auch eure Konzentration und bringt euch zurück ins Hier und Jetzt***. Nehmt euch diese kleinen Auszeiten regelmässig – sie sind ein wertvolles Werkzeug, um eure mentale Gesundheit zu stärken und eure tägliche Arbeit effizienter zu gestalten.

Du kannst Dir das Video mit der geführten Atemübung herunterladen und immer wieder hervor nehmen, wenn Du zwei Minuten Entspannung und Fokus brauchst!

Abbildung 34 - Zusatz: Atemübung für Achtsam durch den Alltag mit Video

Tabelle 2 - Eindrücke Woche 2: SocialEngineering Audioexkurs

6.5 Woche 3: IT-Sicherheit am Arbeitsplatz

6.5.1 TAG 1: Einführung in IT-Sicherheit am Arbeitsplatz

- Was ist Cybersecurity?
- Bedeutung von sensiblen Daten
- Verantwortung jedes Mitarbeiters
- Zusammenfassung Tag 1

6.5.2 TAG 2: Passwortsicherheit

- Erstellung starker Passwörter
- Vermeidung von Passwortdiebstahl
- Zusammenfassung TAG 2

6.5.3 TAG 3: Sicheres Arbeiten im WWW

- Schutz persönlicher Daten
- DeepL, ChatGPT, Google & co.
- Zusammenfassung Tag 3

6.5.4 TAG 4: Sicherheitsrichtlinien und Best Practices

- Einhaltung von Unternehmensrichtlinien
- Quizz Woche 3: IT Security am Arbeitsplatz
- Zusammenfassung Tag 4

6.5.5 TAG 5: Zusammenfassung Woche 3

- Was habe ich gelernt?
- Big Picture
- Abschluss des Kurses

6.5.6 Eindrücke in den Kurs

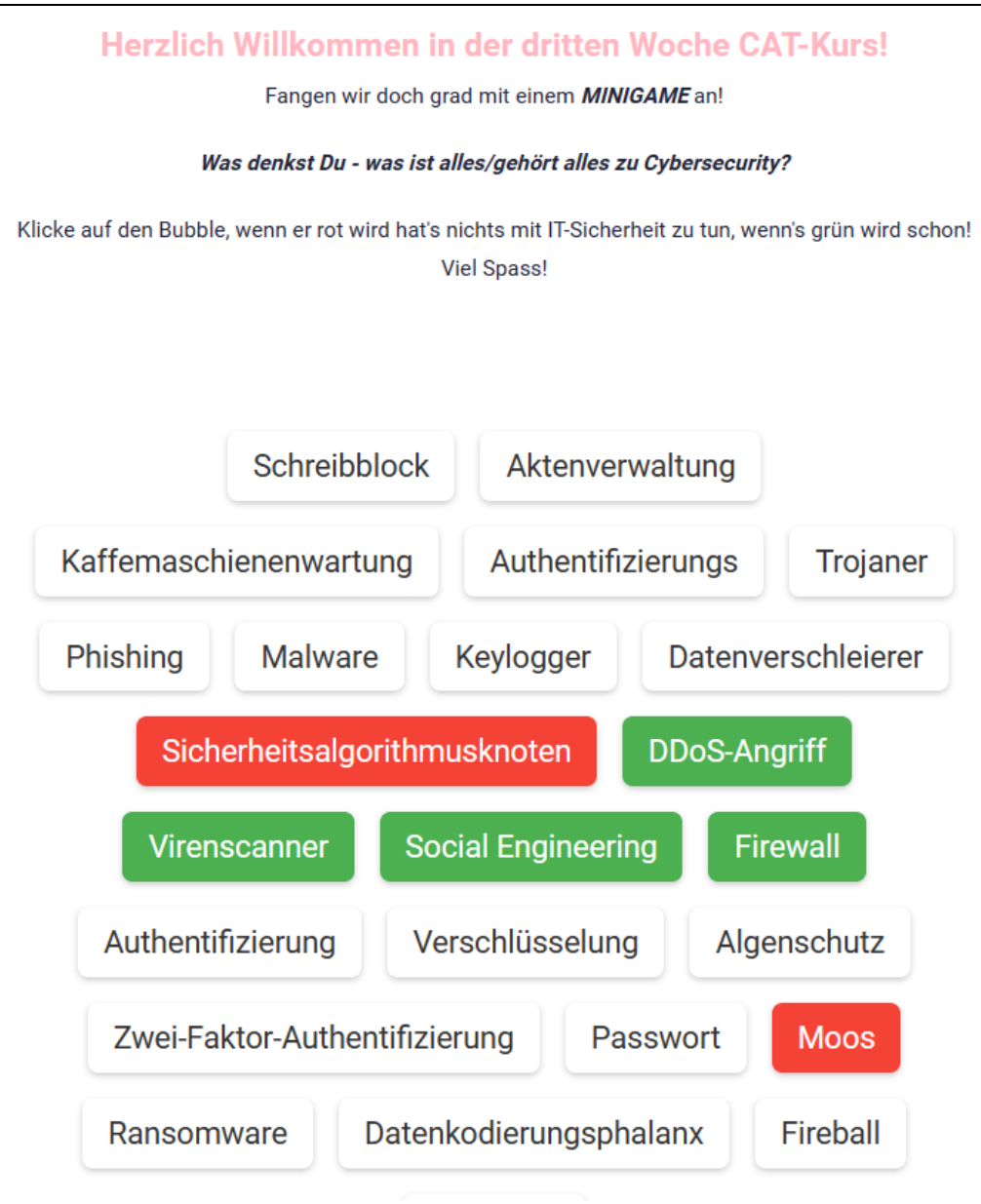


Abbildung 35 - MiniGame "Was ist Cybersecurity"

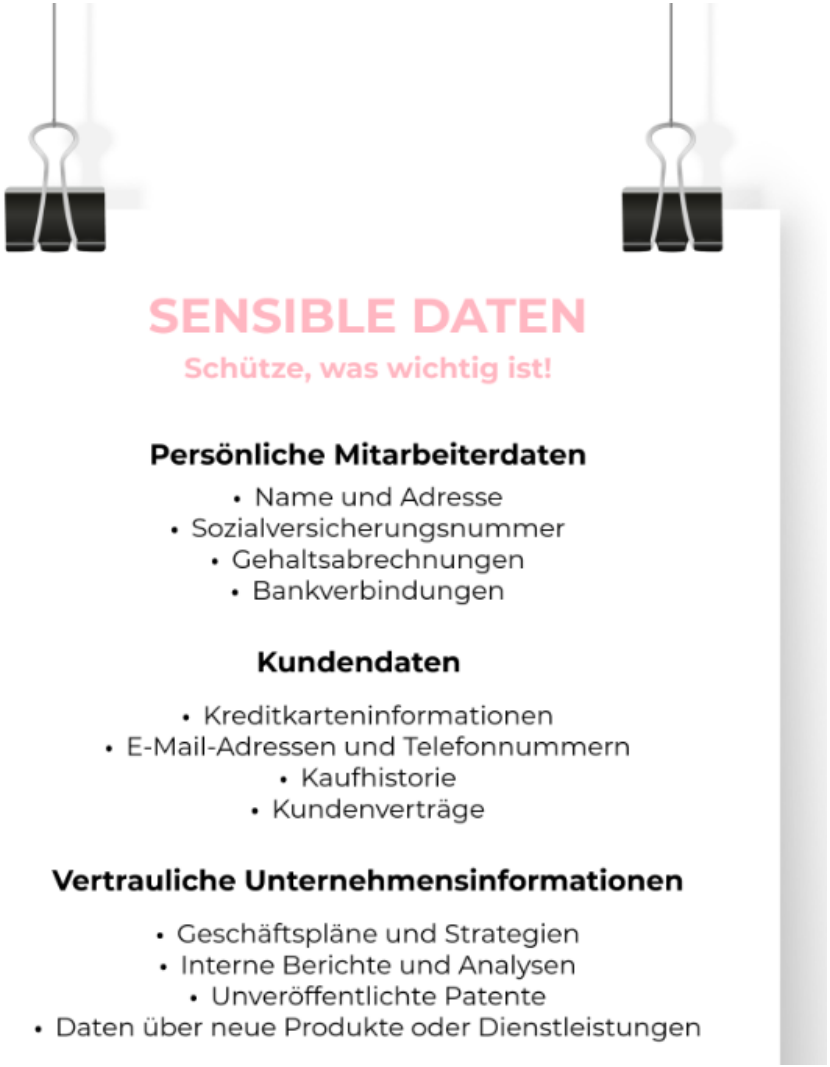


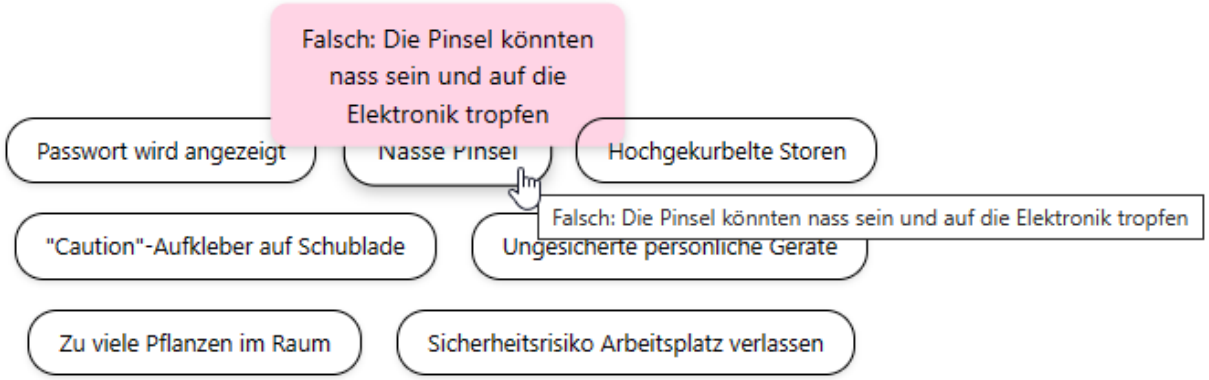
Abbildung 36 - Poster Sensible Daten

Was DU siehst:

Was der HACKER sieht:

Abbildung 37 - Bildbeispiele "Was DU siehst" & "Was der Hacker sieht"

Abbildung 38 - Interaktives Suchspiel "Sicherheitsrisiken"


Falsch: Die Pinsel könnten nass sein und auf die Elektronik tropfen
Passwort wird angezeigt
Nasse Pinsel
Hochgekurbelte Storen
Falsch: Die Pinsel könnten nass sein und auf die Elektronik tropfen
"Caution"-Aufkleber auf Schublade
Ungesicherte persönliche Gerate
Zu viele Pflanzen im Raum
Sicherheitsrisiko Arbeitsplatz verlassen

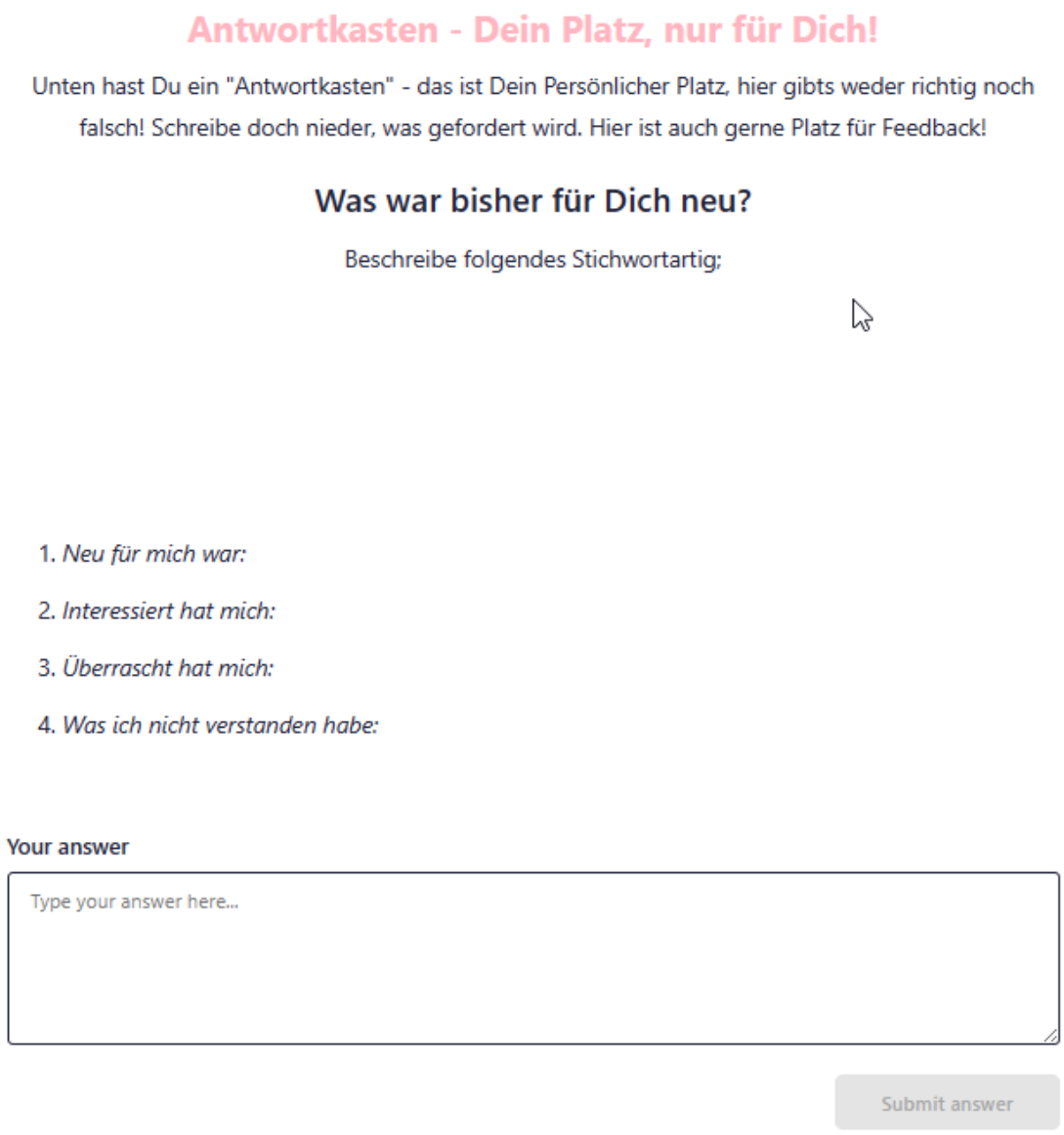


Abbildung 39 - Diverse Antwortkasten

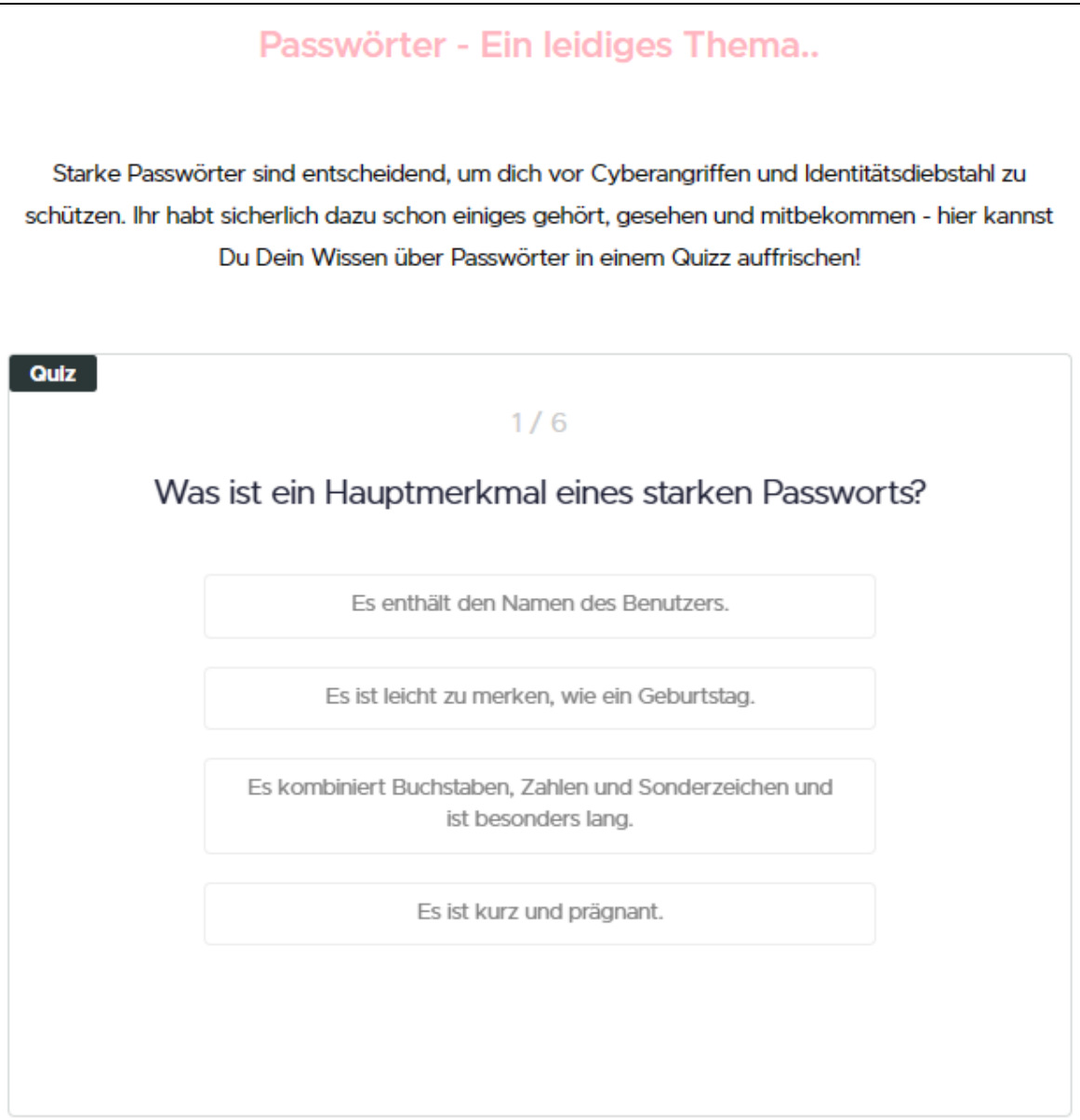


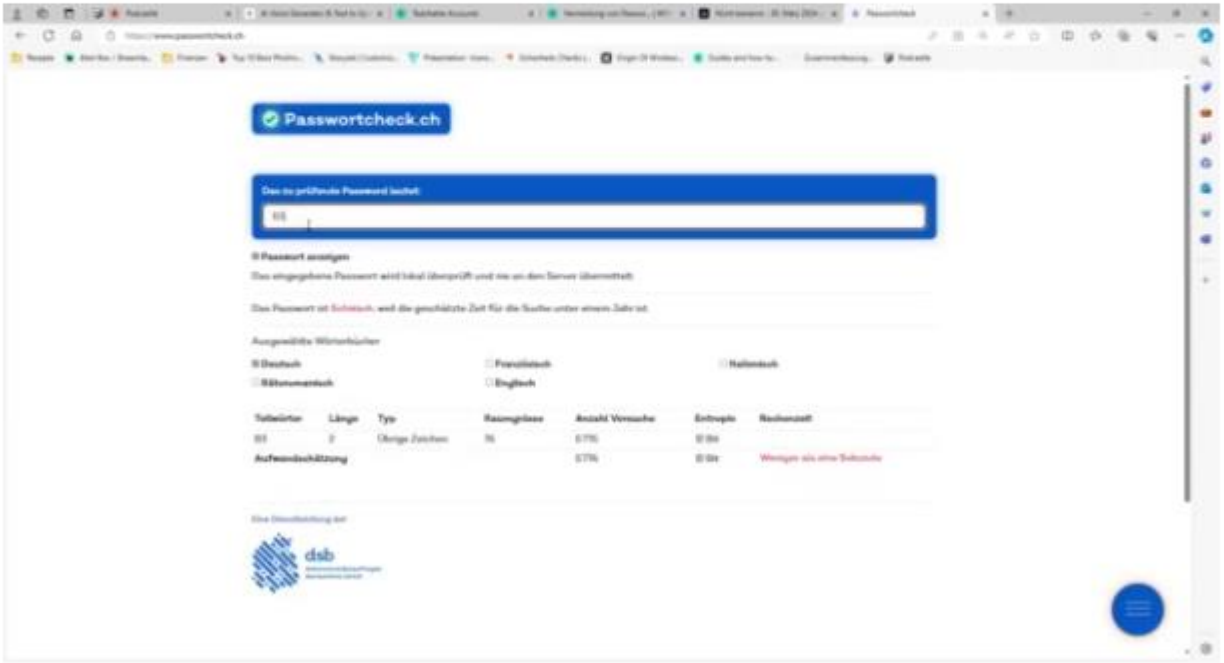
Abbildung 40 - Diverse Quizzes

Wusstest Du.. ***Passwort "B3rl1n88!" ist weniger sicher als "ichginggesternspatzierenundsahvierkatzen".*** "ichginggesternspatzierenundsahvierkatzen" ist länger und komplexer, was es sicherer macht. ***Ein Passwort, das ein vollständiger Satz ist, ist sicherer als ein kurzes Passwort mit Sonderzeichen.*** Längere Passwörter wie vollständige Sätze sind in der Regel sicherer als kurze Passwörter, auch wenn sie Sonderzeichen enthalten.	***Abbildung 41 - Diverse Tipps&Tricks***

Schaue hier wie sicher ein Passwort sein kann und wie lange es geht um dieses zu hacken:

Passwortcheck

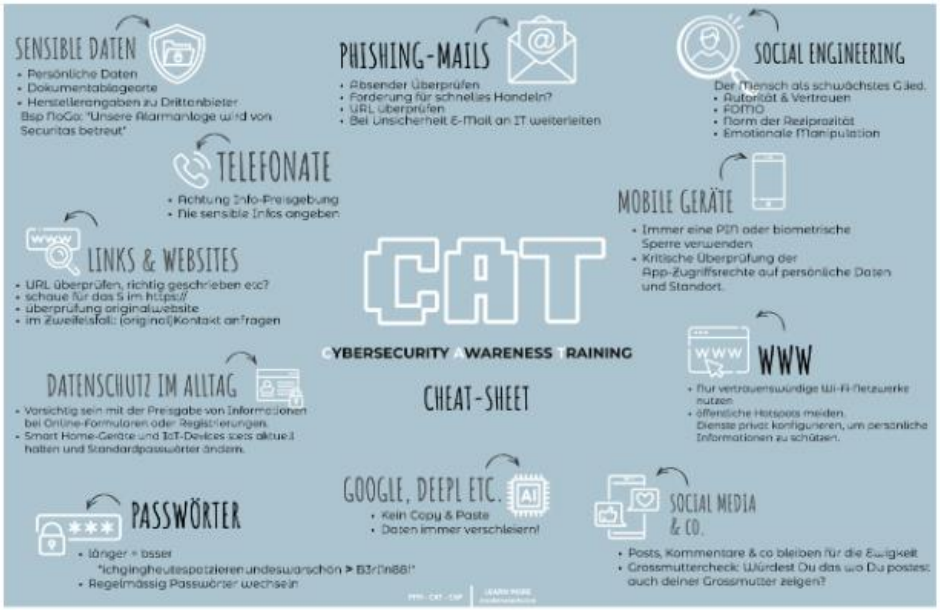
Hier im Video siehst Du drei Passwortbeispiele, siehe sie dir genau an!



Download

Abbildung 42 - Div. Videos mit Tipps& Tricks

Abbildung 43 - Interaktive Zusammenfassungen



Download

Cat_CheatSheet_Blau.png

Abbildung 44 - Big Picture CAT in div. Farben zum Download

Tabelle 3 - Einblicke in Kurs Woche 3: IT-Security am Arbeitsplatz

6.6 CAT-Teachable MJCS Pages

Pro Kurs muss eine sogenannte Sales-Page erstellt werden.

6.7 Digitale Downloads

Es werden diverse digitale Downloads angeboten, entweder direkt in den Kursen, oder als Zusatz auf der CAT-Plattform.

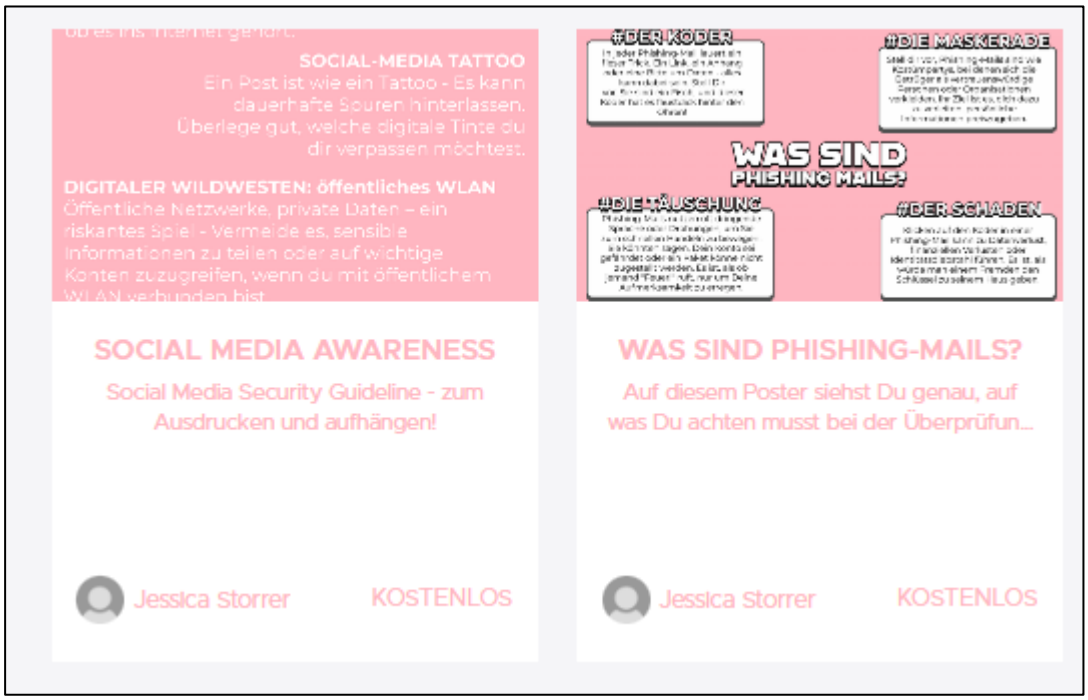


Abbildung 45 - Digitale Downloads

6.8 Sales-Pages

Pro Kurs, Digitaler Download etc, muss eine Sale-Page generiert werden, sodass die User diese Purchasen können. Entweder mit Code oder per Bezahlung. Da man relativ eingeschränkt ist, wurde hier mit Bildern gearbeitet im Header. Diese wurden mit Adobe-Express gestaltet.

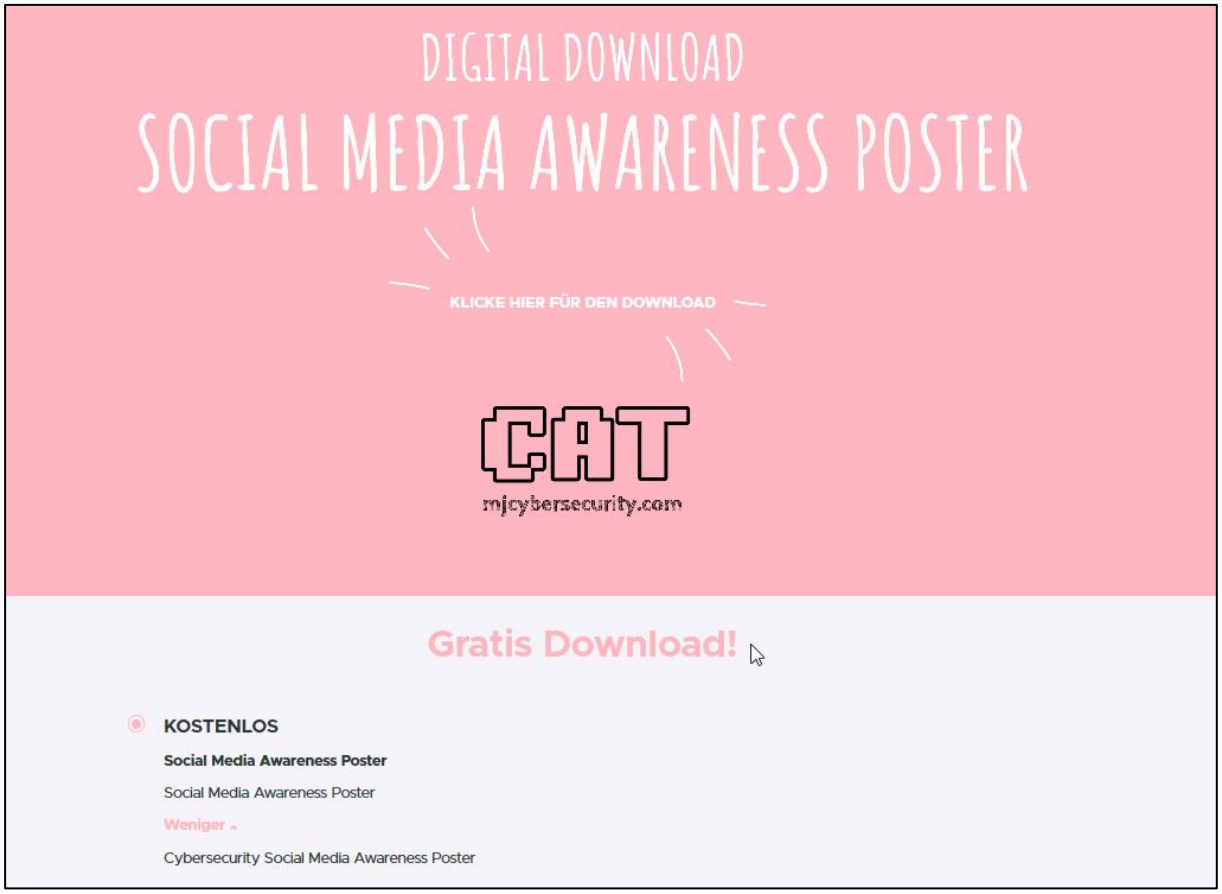


Abbildung 46 - Sales Page "Digitaler Download"

6.9 Achtsamkeit-Zusatz

In der zweiten Woche am letzten Tag gibt es eine Achtsamskeitsübung und eine weitere Übung zur Achtsamkeit und Entspannung als Zusatz.

6.10 CAP (Zusatz)

Als Zusatz wurde eine Pilotfolge des Podcastet CAP – „Cybersecurity Awareness Podcast by Je“. Nach Beendung dieses Projektes ist die zweite Folge geplant, unter anderem aufgrund guten Höhrerfeedbacks.

6.11 Backend

Im Backend werden die Kurse, SalesPages, Reports, etc. generiert und Konfiguriert. In diesem Dokument wird nicht darauf eingegangen, wie ein Kurs erstellt wird. (Selbsterklärend)

6.11.1 Dashboard & Auswertungen

Im Dashboard können alle Neuanmeldungen, Verkäufe, etc. visuell dargestellt werden.

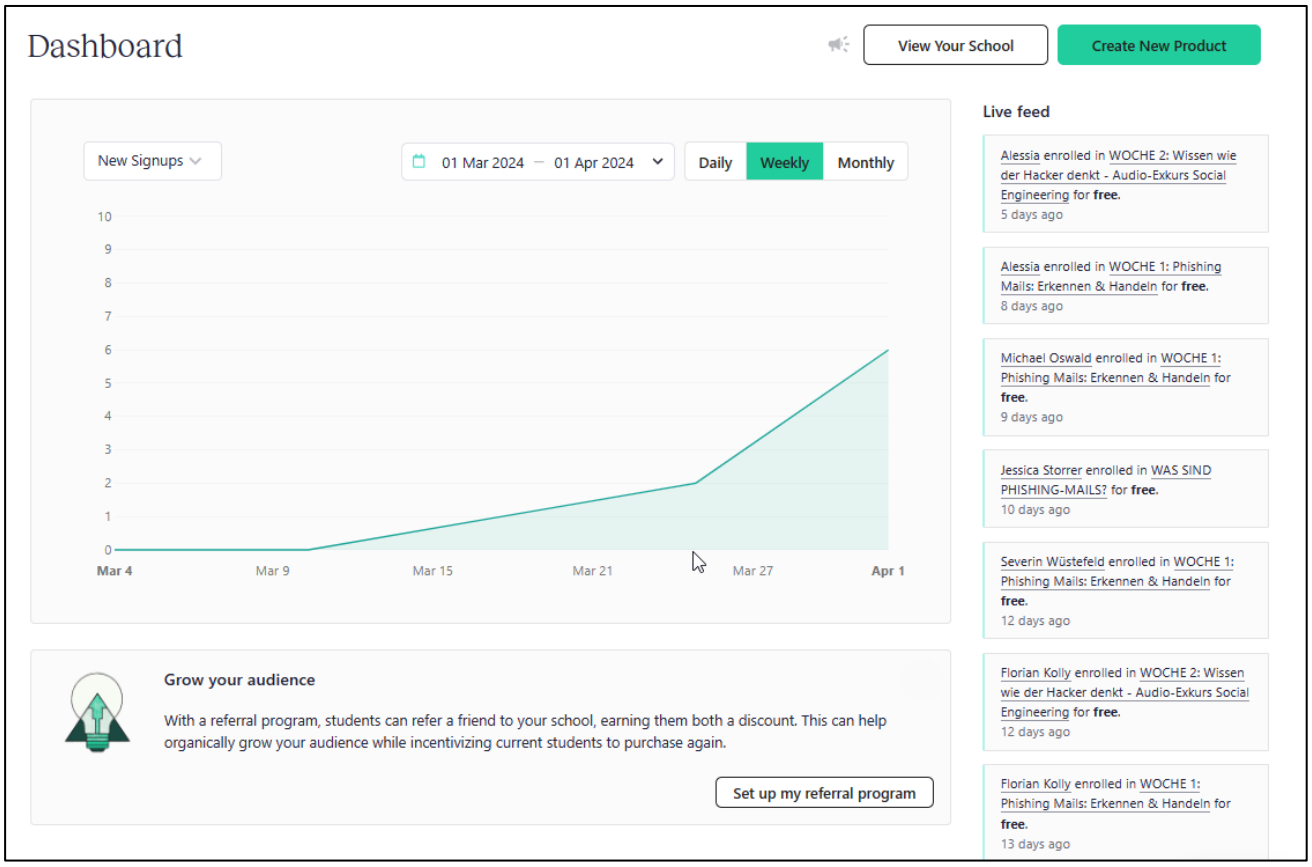


Abbildung 47 - Dashboard Teach:able

Im Kurs wurden diverse „Antwortkasten“ hinterlegt. Die Auswertungen dazu – und weitere Auswertungen – können pro Kurs eingesehen werden. Folgend sind ein paar der Wichtigsten

Reports aufgezeigt. Alle Reports können ebenso für weitere Zwecke als CSV exportiert werden.

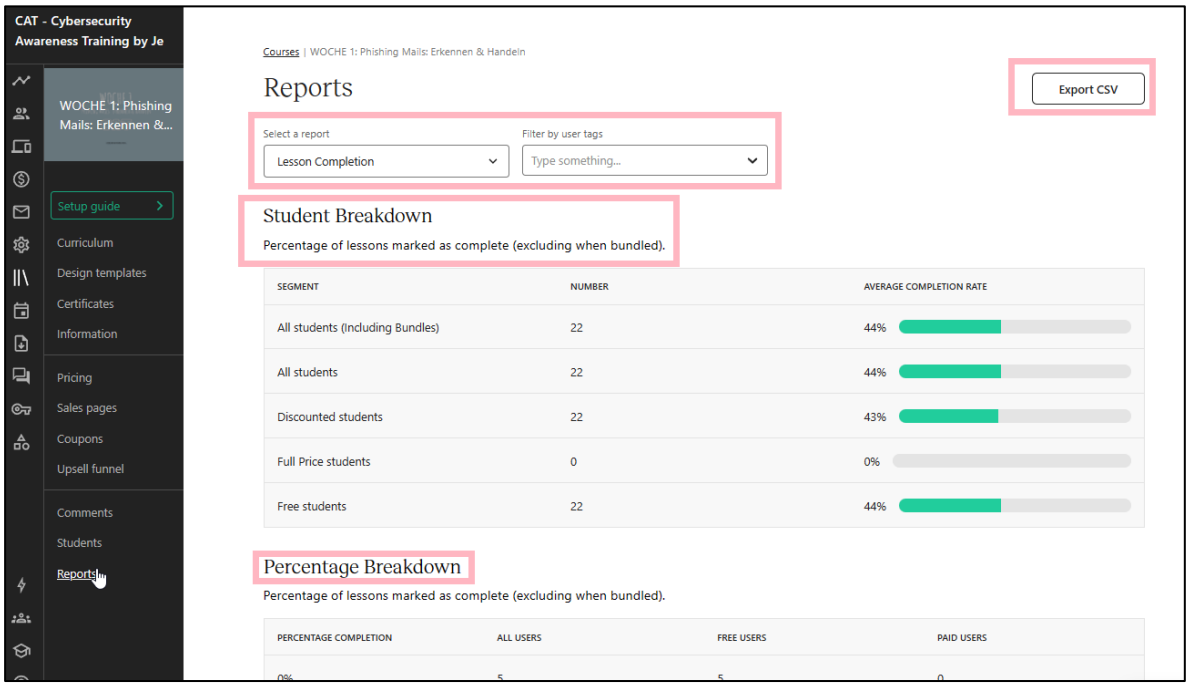


Abbildung 48 – Reportmöglichkeiten

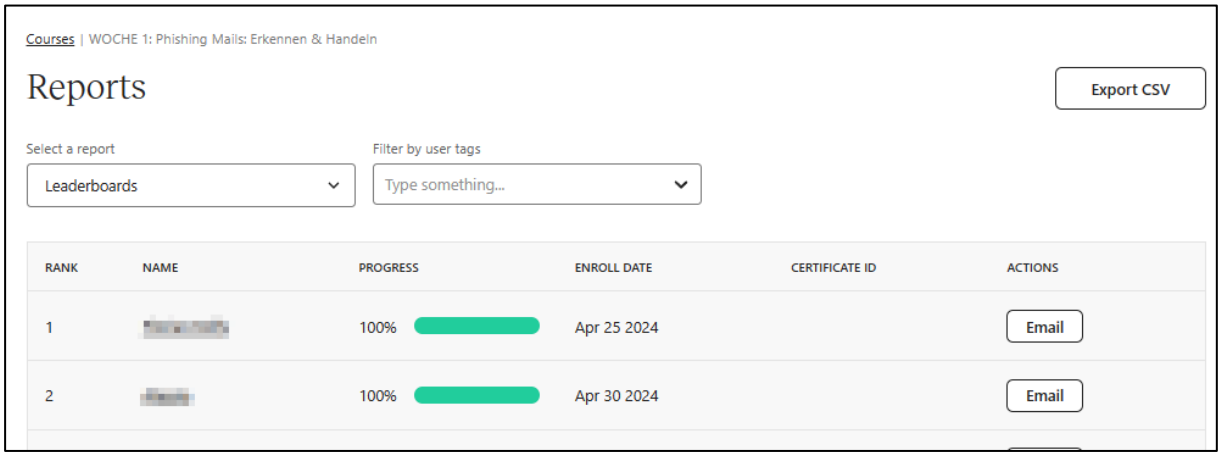


Abbildung 49 - Weitere Reportmöglichkeiten pro Kurs

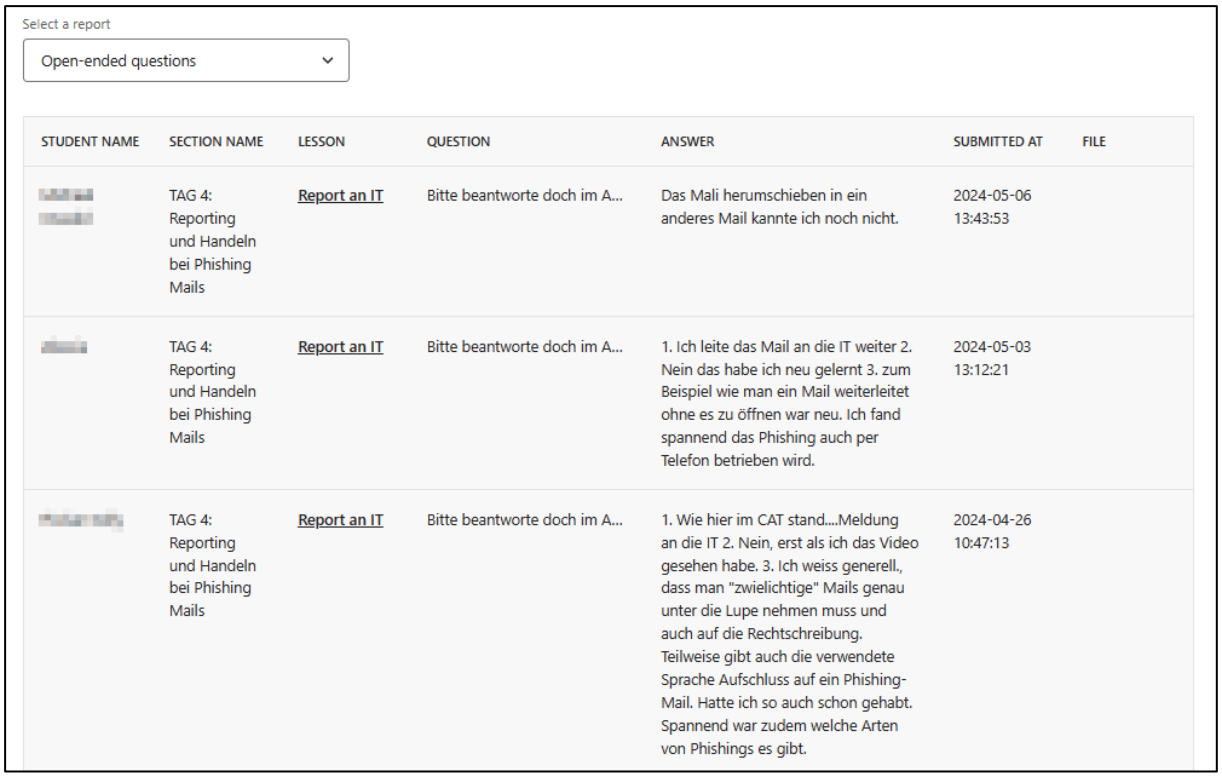


Abbildung 50 - Antwortkasten Reports

7. Abschlussworte Realisierung

Die Realisierung der CAT-Kurse war eine schöne kreative Tätigkeit auf einer super Plattform. Es wird gebeten, falls MJCS neue Mitarbeiter rekrutiert, darauf zu achten, dass die Kursschreibenden und Aufsetzenden genauso kreativ mitwirken wollen.

Ein Kurs zu designen war aufwändiger als gedacht, allemal da man für den User denken muss, welcher eine „non-IT-Person“ ist.

Literaturverzeichnis

Eidesstattliche Erklärung

Mit meiner Unterschrift erkläre ich, dass die vorliegende Arbeit selbständig und nur unter Verwendung der im Literaturverzeichnis aufgeführten Quellen erarbeitet worden ist. Die Stellen meiner Arbeit, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen sind, habe ich in jedem Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht. Die Angaben sind für jede einzelne Quelle als Fussnote mit Verweis auf die Quelle aufgeführt. Dasselbe gilt sinngemäss für Tabellen, Karten und Abbildungen, auch solche, die aus Internetquellen stammen.

Ort, Datum	Unterschrift