Cybersecurity im beruflichen und privaten Alltag

Dr. Michelle Walther |
Themengebiet Digitale Souveränität

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Fokus Mensch



Dr. Michelle Walther

Mittelstand-Digital Zentrum Fokus Mensch

Themengebiet Digitale Souveränität |
Hochschule Bonn-Rhein-Sieg

m.walther@digitalzentrum-fokus-mensch.de

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-
Digital

Mittelstand-Digital
Zentrum
Fokus Mensch

Agenda

1. Das Mittelstand-Digital Zentrum Fokus Mensch
2. Social Engineering
3. (Spear-)Phishing
4. Prävention und Detektion
5. Praxisbeispiele

Mittelstand-Digital
Zentrum
Fokus Mensch

Mittelstand-Digital Zentrum Fokus Mensch

Netzwerk Mittelstand-Digital

Mittelstand-Digital
Zentren
Deutschlandweit

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages



Stand: August 2023

Mittelstand-Digital Zentrum Fokus Mensch

Gemeinsam die digitale Zukunft menschzentriert gestalten.

Menschzentrierte Innovation und Gestaltung
Fraunhofer Institut für Arbeitswirtschaft und Organisation

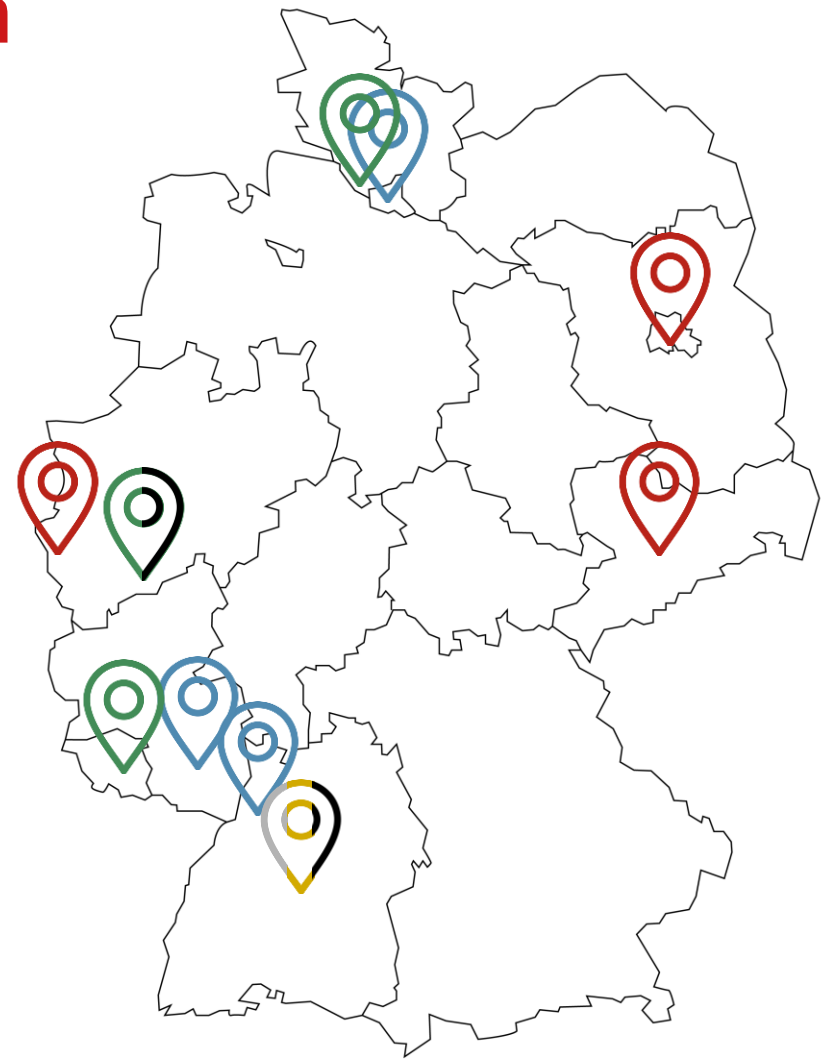
Digitale Souveränität
Hochschule Bonn-Rhein-Sieg
NORDAKADEMIE
Ergosign

Wohlbefinden und Resilienz
Hochschule der Medien Stuttgart

Nachhaltige Transformation
Universität Hamburg
Usability in Germany e. V.
Karlsruher Institut für Technik
Hochschule Kaiserslautern

Fairness und Diversität
Technische Universität Chemnitz
Technische Universität Berlin
BITMi e. V.

Künstliche Intelligenz
Hochschule Bonn-Rhein-Sieg
Hochschule der Medien Stuttgart



Grafik angelehnt an Bruce Jones Design Inc. auf freeusandworldmaps
Icons von Freepik und Mayor Icons auf Flaticon.com

Mittelstand-Digital
Zentrum
Fokus Mensch

Cybersecurity im beruflichen und privaten Alltag

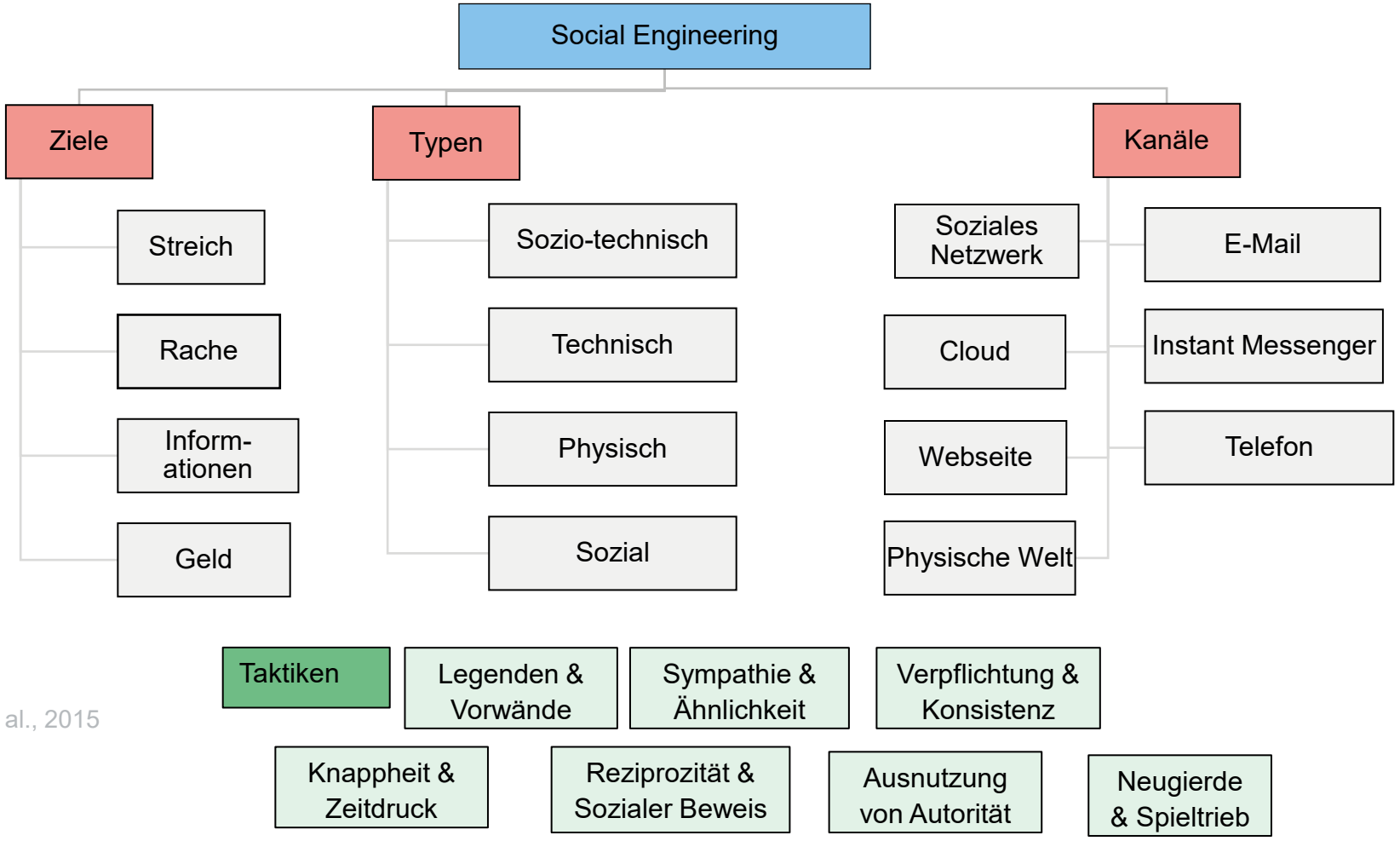
Mittelstand-Digital
Zentrum
Fokus Mensch

Social Engineering

Social Engineering

- Falsche Identität wird angenommen, um wahren Absichten zu verbergen (Fox 2014)
- Gezieltes Ausnutzen menschlicher Bedürfnisse und pro-soziales Verhaltensweisen (Nohlberg 2008; Nohlberg und Kowalski 2008)

Social Engineering Taxonomie



nach Krombholz et. al., 2015

Prozessmodell



- Auswahl des Opfers und der Infos (Crawling mit KI)



- Durchführung (Design & Kommunikation mit KI)



- Verschleierung (Kommunikation mit KI)

Mittelstand-Digital
Zentrum
Fokus Mensch

Wie Ihre Daten Attacken füttern

Öffentliche Informationen

- Social-Media-Profile und andere Online-Informationen scannen, um personalisierte Angriffe zu erstellen – Spear-Phishing
  - Lieblingsmarken die Ihnen Gutscheine anbieten
  - DHL weil Sie etwas online bestellt haben
  - Sicherheitsabbos und –software
  - Urlaub nutzen um einzubrechen oder bei Ihren Kunden in Ihrem Namen anzurufen
- KI nutzen um legitime Kommunikation nachzuahmen (z.B. HTML-Design)



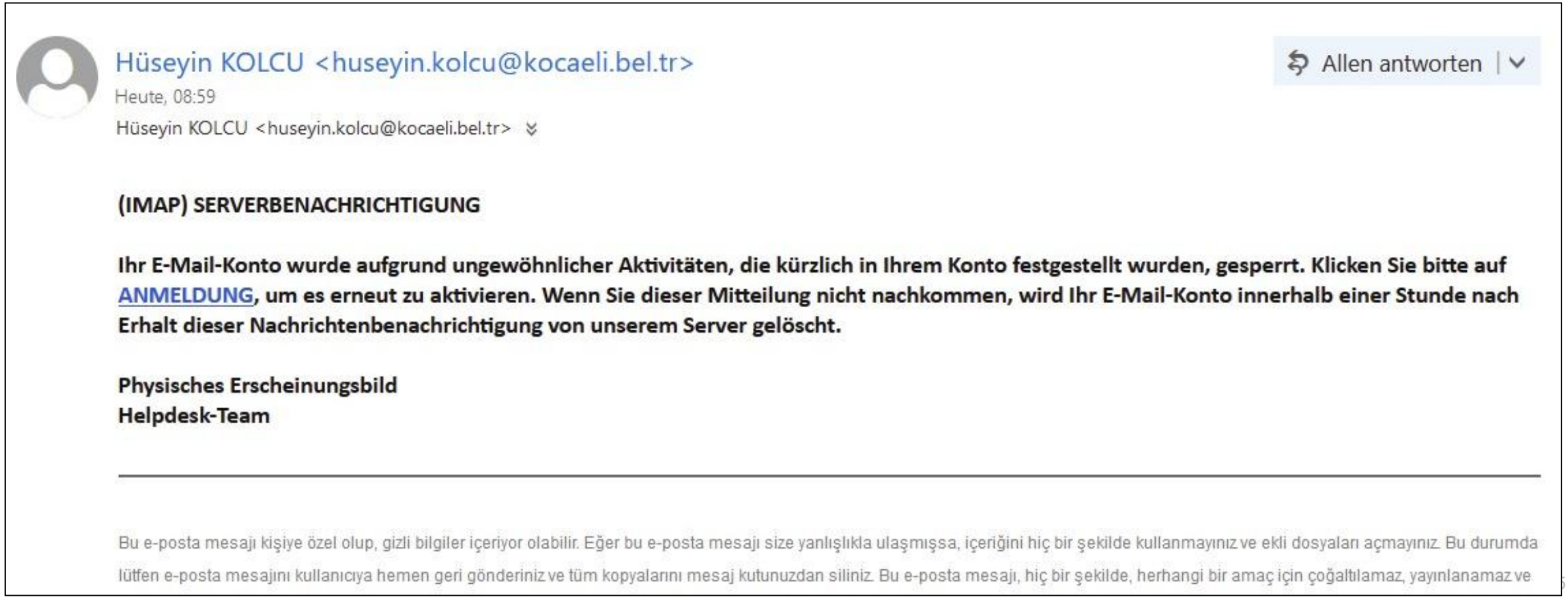
Mittelstand-Digital
Zentrum
Fokus Mensch

(Spear-)Phishing

Mittelstand-Digital
Zentrum
Fokus Mensch

Phishing Definition

- Betrug um persönliche Informationen der Benutzer zu stehlen, z.B. Anmeldedaten für den Zugang zu geschützten Systemen (Dhamija, Tygar, und Hearst, 2006)



Hüseyin KOLCU <huseyin.kolcu@kocaeli.bel.tr>
Heute, 08:59
Hüseyin KOLCU <huseyin.kolcu@kocaeli.bel.tr>

Allen antworten

(IMAP) SERVERBENACHRICHTIGUNG

Ihr E-Mail-Konto wurde aufgrund ungewöhnlicher Aktivitäten, die kürzlich in Ihrem Konto festgestellt wurden, gesperrt. Klicken Sie bitte auf ANMELDUNG, um es erneut zu aktivieren. Wenn Sie dieser Mitteilung nicht nachkommen, wird Ihr E-Mail-Konto innerhalb einer Stunde nach Erhalt dieser Nachrichtenbenachrichtigung von unserem Server gelöscht.

Physisches Erscheinungsbild
Helpdesk-Team

Bu e-posta mesajı kişiye özel olup, gizli bilgiler içeriyor olabilir. Eğer bu e-posta mesajı size yanlışlıkla ulaşmışsa, içeriğini hiç bir şekilde kullanmayınız ve ekli dosyaları açmayınız. Bu durumda lütfen e-posta mesajını kullanıcıya hemen geri gönderiniz ve tüm kopyalarını mesaj kutunuzdan siliniz. Bu e-posta mesajı, hiç bir şekilde, herhangi bir amaç için çoğaltılamaz, yayınlanamaz ve

Phishing als Kanal

- Verschiedene Formen von Onlinebetrug (Button & Cross, 2017)
  - Produkt- /Dienstleistungsbetrug
  - Identitätsbetrug
  - Gewinnspiel- und Preis-Betrug
  - Wohltätigkeitsbetrug



Kontaktieren Sie uns für Ihr verlorenes Geld

Linda Lizzy <service@inflowrenuity.pro>
Mo 22.04. 13:19
[redacted]

Allen antworten

Hallo [redacted]

Wir freuen uns, Ihnen mitteilen zu können, dass Ihr ROI (Return of Investment) zur Verarbeitung auf Ihrer Anlageplattform bereit ist. Bitte kontaktieren Sie uns, um die Details des Anlageportfolios zu besprechen.

Ihre Verluste und Erlöse wurden in unsere Kasse eingezahlt und wir verfügen derzeit über Ihre Subventionsrücklage.

Bitte wenden Sie sich an die SWIFT INTERNATIONAL FINANCE BANK und eröffnen Sie dort ein Konto, um Ihre Rückerstattung einzuzahlen.

Ihre Einzahlungsanfrage-ID: 40010203074INC

Kontaktieren Sie uns für weitere Fragen ODER folgen Sie den Anweisungen auf ihrer Website, um ein Konto bei SWIFT INTERNATIONAL FINANCE BANK zu eröffnen, oder kontaktieren Sie unsere Finanzexperten per E-Mail und antworten Sie für weitere Richtlinien und den Auszahlungsprozess oder suchen Sie auf Google (Swift int Finance) und folgen Sie dem Link zu mit der Bank kommunizieren.

Wenn Sie glauben, dass es sich hierbei um einen Fehler handelt, teilen Sie uns dies bitte mit und wir werden ihn beheben.

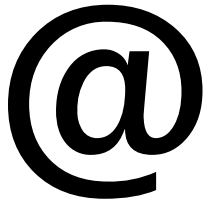
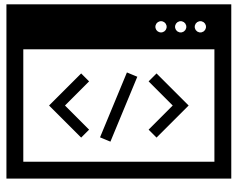
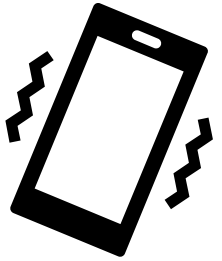
Grüße,

Linda Lizzy

Rückerstattung für Verbraucher

...

Mittelstand-Digital
Zentrum
Fokus Mensch

Phishing



Social Networking

E-Mail von der Social Media Platform, Freundschaftseinladungen, senden eines URL



Spear Phishing

Gezielte Phishing E-Mail im Layout des Arbeitgebers



Spoofed URLs

z.B. in E-Mails

Spoofing Mobile Browsers und Embedded Web Contents

URL wird geklont und verborgen

Mittelstand-Digital
Zentrum
Fokus Mensch

Spear-Phishing



Gezielte Angriffe auf Organisationen und Firmen



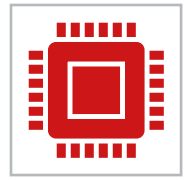
Hoher Aufwand



Schwierig zu erkennen



Kommt oft „aus den eigenen Reihen“



Oft in Kombination mit Spoofing

Mittelstand-Digital
Zentrum
Fokus Mensch

Prävention vs. Detektion

Protection Motivation Theory

- Äußere und innere Faktoren können die Entstehung von zwei unterschiedlichen kognitiven Prozessen beeinflussen
- **Bedrohungseinschätzung**
- **Bewältigungsbedeutung**



https://www.runtervomgas.de/aktuelles-und-downloads/aktuelles/die-autobahnplakate-2020/

Risiko niedrig, die Verwundbarkeit gering oder das Selbstvertrauen niedrig = Motivation gering

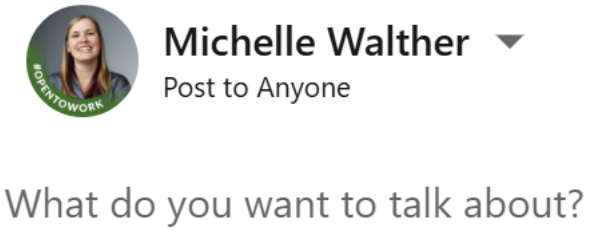
Risiko sehr hoch & Wirksamkeit von Schutzmaßnahmen niedrig = Lähmung

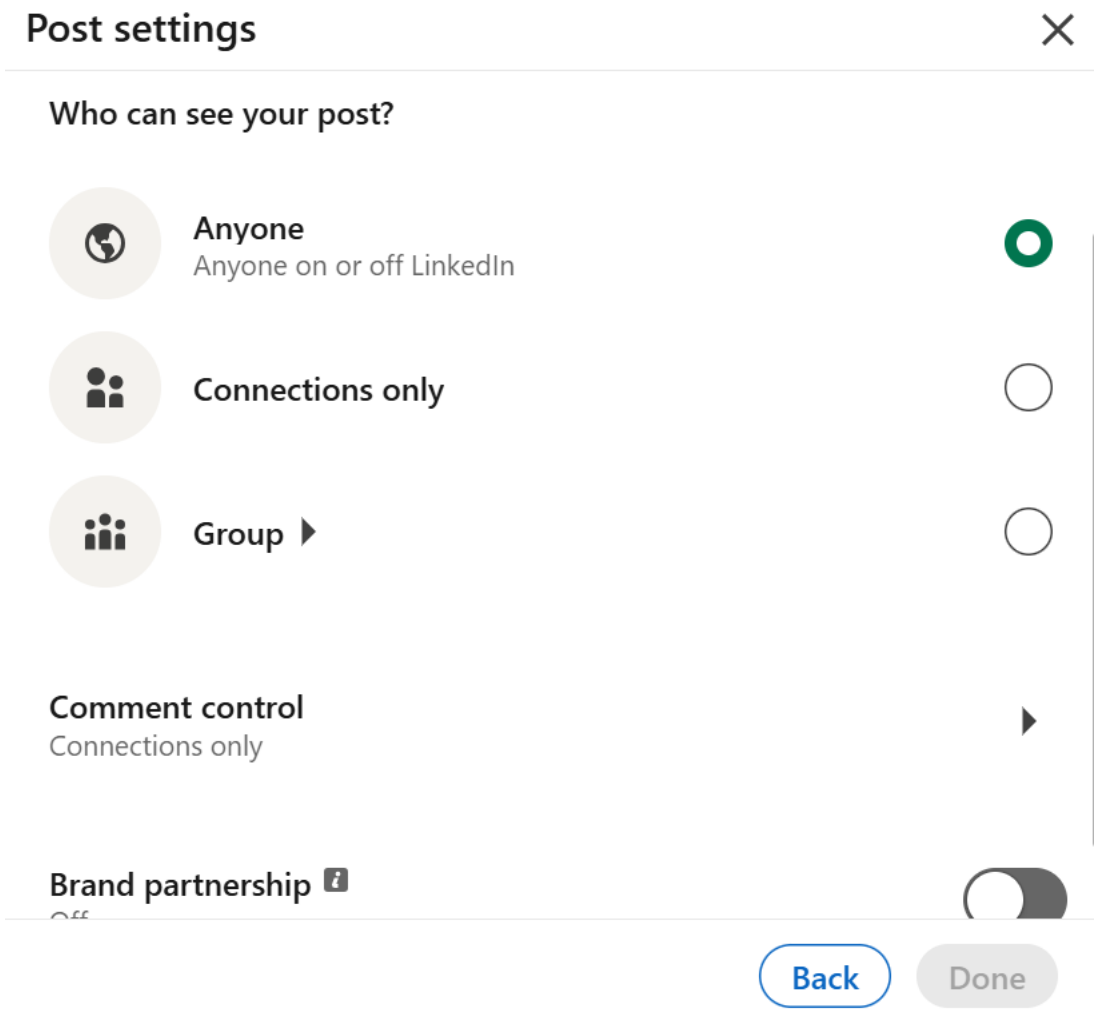
➢ Zielgruppe muss genau bekannt sein

Mittelstand-Digital
Zentrum
Fokus Mensch

Prävention: Datenschutz

- Datenschutz im privaten und beruflichen Alltag
- Inhalte von Fotos
- Daten zu Urlaub, Routinen, Lieblingsmarken, Geschäftsreisen/-treffen
- E-Mail-Adressen
- Telefonnummern
- E-Mail Zertifikate gegen Spear-Phishing
- Chatbots





Datenschutz: Fragen

- Würde ich diese Information einem Fremden auf der Straße erzählen?
- Würde ich diese Information einem konkurrierendem Unternehmen erzählen?
- Kann diese Information gegen mich verwendet werden?
- Hat diese Information etwas mit der Sicherheit meiner Person oder meinem Unternehmen zu tun?
- Was würde ich mit dieser Information anfangen, wenn Sie von jemand anderem kommen würde?

Vorbeugung

- Zwei/Mehr-Faktor-Authentifizierung / Passkey
- Sicherheitsupdates
- Firewall und Sicherheitssoftware
- Sensibilisierung der Mitarbeitenden
  - Persönliche Sicherheitsmaßnahmen
  - Offene Unternehmenskultur & Wachsamkeit im Unternehmen
- Aktuelle Liste von Notfallkontakten für schnelle Verifizierung
  - Bei Zweifel verifizieren, um die Echtheit sicherzustellen

Phishing Detektion

- **Dringender Handlungsbedarf**: "Wenn Sie Ihre Daten nicht umgehend aktualisieren, dann gehen sie unwiederbringlich verloren“ (BSI, 2022)
- **Drohungen**: „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren …" (BSI, 2022)
- Sie sollen vertrauliche Daten wie die PIN für Ihren Online-Bankzugang oder eine Kreditkartennummer eingeben (BSI, 2022)
- Die E-Mail enthält Links oder Formulare (BSI, 2022; Fette et al., 2007)
  - Die URL des Hyperlinks stimmt nicht mit der echten URL der Organisation überein (Singh et al., 2019; Fette et al., 2007)
  - Es sind mehrere Links in der Email enthalten (Fette et al., 2007; Ma et al., 2009)
- Die E-Mail scheint von einer bekannten Person oder Organisation zu stammen, die **E-Mail-Adresse** ist aber eine andere (BSI, 2022)
- Der Text hat kein bestimmtes Layout und/oder HTML (Fette et al., 2007)
- Die Email hat eine undefinierte Anrede

Worauf sollten Betriebe achten?

- Datenschutz
- Workshops
- Poster
- Kampagnen
- Nap Attacken (Ethische Hacker)
- Online Kurse
- Anti-Spam filter etc.
- Entstressen
- Business Contiuity Plan

Digitale Resilienz – Business Continuity Plan

- IT - Notfallkarte vom BSI (bund.de)
- Plan für Worst-case scenario: Wir wurden gehackt
  - Wie wird Kommuniziert?
  - An wen wird Kommuniziert?
  - Back-ups auf externen Festplatten?
  - Wie läuft das Geschäft weiter?
  - Wo muss ich mich melden wenn ich ein Datenleck habe?



VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Mittelstand-Digital
Zentrum
Fokus Mensch

Praxisbeispiele Phishing

PayPal

Kundenmitteilung - Ihre Eingabe ist erforderlich!
Datum: 14.07.2020

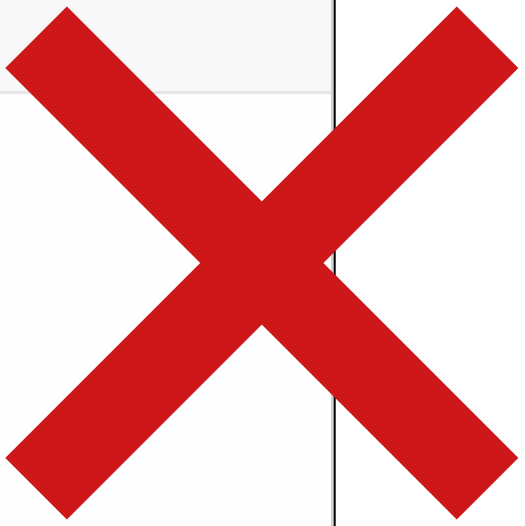
Wichtige Überprüfung! - Ihr Nutzerzugang wurde deaktiviert!

Sehr geerhter Kunde/in,

bei einer Routineüberprüfung ist uns aufgefallen, das Ihr Nutzerkonto ohne Ihr Wissen benutzt wurde. Unser Automatisches System hat nun den Zugang für Sie für Sie nun eingeschränkt. Um Ihr Nutzerkonto wieder wie gewohnt nutzen zu können müssen Sie Ihre persönlichen Daten erneut bestätigen.

Klicken Sie auf "Zum Benutzerlogin" um Ihr Konto zu bestätigen.

Zum Benutzerlogin



Mit feundlichen Grüßen

Ihr Kundenservice Team

Extern Möglichkeit zur Projektfinanzierung – Investoren aus den VAE

PF

Project Financing Consultant <commercialfab.srl@gmail.com>
To

Reply | Reply All | Forward | ...

Do 15.10.2026 10:53

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
We converted this message into plain text format.

Sehr geehrte Damen und Herren,

ich schreibe Ihnen, um Sie auf eine aktuelle Finanzierungsmöglichkeit für Projekte aufmerksam zu machen, die von einer renommierten Investorengruppe mit Sitz in den VAE angeboten wird.

Die Investoren sind bereit, Projekte zu finanzieren, die in ihre festgelegten Finanzierungskategorien fallen. Die Zinssätze beginnen bereits bei 2 % – vorbehaltlich der Eignung des Projekts, einer entsprechenden Sorgfaltsprüfung (Due Diligence) sowie der Vereinbarung der Finanzierungsbedingungen.

Ich bin als Berater für diese Investoren tätig und kann Sie – gemeinsam mit deren Finanzierungsgesellschaft – bei der Einreichung Ihres Vorhabens sowie bei der Sicherung der Finanzierung für geeignete Projekte unterstützen.

Sollten Sie aktuell ein Projekt haben, für das eine Finanzierung benötigt wird, stelle ich Ihnen gerne weitere Informationen zur Finanzierungsstruktur, zu den Anforderungen, den Zulassungsvoraussetzungen sowie zum Antragsverfahren zur Verfügung.

Kontaktieren Sie mich gerne, wenn Sie Ihr Projekt besprechen oder mehr über diese Finanzierungsmöglichkeit erfahren möchten.

Ich freue mich darauf, von Ihnen zu hören.

Mit freundlichen Grüßen
Charles Rix
Berater für internationale Finanzierung und Projektfinanzierung

Baldiger Ablauf Ihrer sciebo-Nutzungsberechtigung / Expiration of your ...

info@sciebo.de
An Walther, Michelle
01:52
Signiert von info@sciebo.de

English version below

Sehr geehrte*r Michelle Walther,

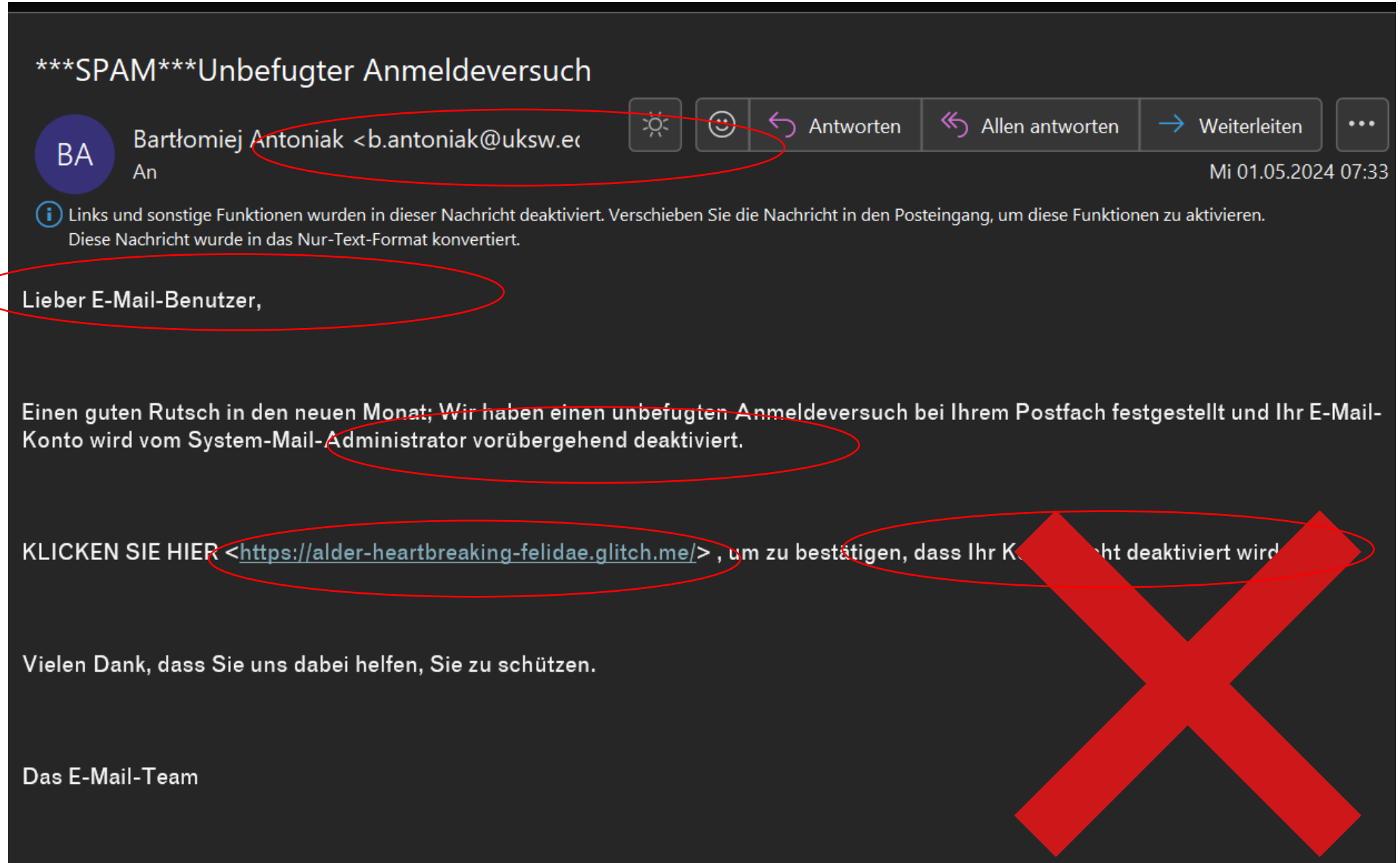
Ihr sciebo-Account "michelle.walther@h-brs.de" läuft am 13.08.2024 ab.

Um Ihren sciebo-Account weiternutzen zu können, müssen Sie es für ein Jahr verlängern. Das ist ganz einfach möglich, indem Sie den Link https://www.sciebo.de/verlaengerung nutzen und sich dort mit der zentralen Kennung Ihrer Einrichtung (nicht Ihrer sciebo-Kennung) einloggen.

Falls Sie Ihren Account nicht verlängern, wird er nach einer Kulanzfrist gelöscht. In diesem Fall sichern Sie bitte Ihre Daten vorab. Lokal auf Ihren Endgeräten synchronisierte Daten bleiben selbstverständlich erhalten. So lange Sie einer an sciebo teilnehmenden Einrichtung angehören, können Sie sich jederzeit wieder für sciebo registrieren.

Bei Fragen hierzu antworten Sie nicht auf diese E-Mail, sondern verwenden Sie unser Kontaktformular:
https://www.sciebo.de/de/kontakt/index.html

Mit freundlichen Grüßen
Ihr sciebo-Team



SPAMUnbefugter Anmeldeversuch

BA

Bartłomiej Antoniak <b.antoniak@uksw.e

An

Antworten | Allen antworten | Weiterleiten | ...

Mi 01.05.2024 07:33

Links und sonstige Funktionen wurden in dieser Nachricht deaktiviert. Verschieben Sie die Nachricht in den Posteingang, um diese Funktionen zu aktivieren.
Diese Nachricht wurde in das Nur-Text-Format konvertiert.

Lieber E-Mail-Benutzer,

Einen guten Rutsch in den neuen Monat; Wir haben einen unbefugten Anmeldeversuch bei Ihrem Postfach festgestellt und Ihr E-Mail-Konto wird vom System-Mail-Administrator vorübergehend deaktiviert.

KLICKEN SIE HIER <https://alder-heartbreaking-felidae.glitch.me/> , um zu bestätigen, dass Ihr K ht deaktiviert wird

Vielen Dank, dass Sie uns dabei helfen, Sie zu schützen.

Das E-Mail-Team

Erforderliche Aktion: Benutzersicherheitswarnung

Marta Kowalenko <m.kowalenko@uksw.edu.pl>
Mi 08.05, 07:58

Allen antworten

Hallo E-Mail-Benutzer

Aufgrund des erhöhten Datenverkehrs in unserer Internetdatenbank werden wir alle nicht verwendeten E-Mails löschen, um Speicherplatz freizugeben. Wenn Sie Ihr Konto weiterhin bei uns behalten möchten, müssen Sie Ihr Konto innerhalb von 72 Stunden nach Erhalt dieser Mitteilung aktualisieren.

HIER KONTO AKTUALISIEREN.

Andernfalls gehen wir davon aus, dass Sie kein Interesse daran habe bei uns zu führen. Ihr E-Mail-Konto wird dauerhaft gesperrt und sein gesamter Inhalt wird gelöscht.

Vielen Dank, dass Sie uns helfen, Sie zu schützen.

Beste grüße,
Das Mail-Team



Anstehende Veranstaltungen im Zentrum

18.11.2026: Digitale Zukunft gemeinsam gestalten
Was brauchen Organisationen heute? Was brauchen Engagierte morgen?
Betahaus, Hamburg, 13:30-20:00 Uhr

09.12.2026: Let me “Feldanalyse” that for you! – Feldanalyse KI
Online, 08:30-09:00 Uhr

09.12.2026: KI-Use-Cases richtig verstehen
Bedarfsanalyse und Priorisierung am Beispiel einer Arztpraxis
Online, 17:00-18:00 Uhr



Foto von freepik auf freepik.com

DANKE

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

Wie war‘s? Ihr Feedback zählt!



Foto von Kelly Sikkema auf Unsplash

Mittelstand-Digital
Zentrum
Fokus Mensch



Dr. Michelle Walther

Mittelstand-Digital Zentrum Fokus Mensch

Themengebiet Digitale Souveränität |
Hochschule Bonn-Rhein-Sieg

m.walther@digitalzentrum-fokus-mensch.de