



Schulung „Cyber-Sicherheit“

06. Februar 2025

1. Einleitung

Ziele der Schulung

- **Bewusstsein für Cyber-Bedrohungen schaffen**
 - Vermittlung eines grundlegenden Verständnisses für die Bedeutung von Cyber-Sicherheit
 - Sensibilisierung für typische Gefahren im Arbeitsalltag (Pishing, Malware, Social Engineering)
- **Praktische Tipps für den sicheren Umgang mit IT-Systemen vermitteln**
 - Konkrete Anweisungen, wie Sicherheitsrisiken in den Arbeitsalltag
 - Integration von Sicherheitsrichtlinien in den Arbeitsalltag
- **Verantwortung jedes Einzelnen betonen**
 - Jeder Mitarbeiter ist ein entscheidender Faktor für die Sicherheit der Organisation
 - Fehlverhalten kann zu erheblichen Risiken führen

1. Einleitung

Bedeutung von Cyber-Sicherheit

- Wachsende Anzahl an Cyber-Angriffen
 - Laut aktuellen Studien steigen Cyber-Angriffe weltweit rasant an
 - Angriffe sind nicht nur auf grosse Unternehmen beschränkt, sondern treffen auch kleinere Organisation (BEKB, TFBO, HTR, Rugenbräu AG)
- Beispiele für reale Fälle & Folgen (Datenverlust)
 - Ein Mitarbeiter öffnet einen Pishing-Link, wodurch vertrauliche Kundendaten kompromittiert werden
 - Folgen: Vertrauensverlust, rechtliche Konsequenzen und finanzielle Einbussen
- Beispiele für reale Fälle & Folgen (Finanzielle Schäden)
 - Ransomware-Angriffe, bei denen Organisationen Lösegeld zahlen mussten, um Daten wiederherzustellen
 - Folgen: Hohe Kosten und Betriebsunterbrechungen

2. Grundprinzipien der Cyber-Sicherheit

Starkes Passwort-Management

- Anforderungen an sichere Passwörter
 - Mindestens 12 Zeichen
 - Kombination aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen
 - Keine Wiederverwendung alter Passwörter
 - Vermeidung persönlicher Informationen (z.B. Geburtsdatum, Namen von Familienmitgliedern)
- Verwendung von Passwort-Managern
 - Speicherung und Verwaltung von Passwörtern in einer sicheren Umgebung
 - Automatische Generierung sicherer Passwörter
- Regelmässiges Ändern von Passwörtern
 - Mindestens alle 3 Monate
 - Passwörter sofort ändern, wenn ein Sicherheitsvorfall vermutet wird

2. Grundprinzipien der Cyber-Sicherheit

Vorsicht vor Phishing und Social Engineering

- Merkmale von Phishing E-Mails
 - Gefälschte Absenderadressen (z.B. leichte Abweichungen von echten Domains)
 - Grammatik- und Rechtschreibfehler
 - Dringlichkeit oder Drohungen (z.B. „Ihr Konto wurde gesperrt“)
 - Aufforderung auf Links zu klicken oder Anhänge zu öffnen
- Umgang mit verdächtigen Links oder Anhängen
 - Keine Links in E-Mails anklicken, wenn der Absender nicht eindeutig vertrauenswürdig ist
 - Anhänge nur öffnen, wenn sie erwartet werden und aus einer sicheren Quelle stammen
 - Verdächtige E-Mails sofort dem IT-Verantwortlichen melden
- Praxisübung: Erkennen einer Phishing E-Mail
 - Beispiele analysieren von echten und gefälschten E-Mails
 - Welche Hinweise machen die gefälschte E-Mail erkennbar?

2. Grundprinzipien der Cyber-Sicherheit

Software-Updates und Patches

- Warum Updates wichtig sind
 - Schliessen von Sicherheitslücken in Betriebssystemen und Anwendungen
 - Schutz vor bekannten Schwachstellen, die von Cyber-Kriminellen ausgenutzt werden
- Automatische Updates aktivieren
 - Anleitung, wie automatische Updates auf Betriebssystemen (z.B. Windows, macOS) und Anwendungen aktiviert werden
 - Wichtigkeit von Updates für Antiviren-Programme und Sicherheitssoftware
 - Verdächtige E-Mails sofort dem IT-Verantwortlichen melden

3. Praktischer Umgang mit Sicherheitsrichtlinien

E-Mail-Sicherheit

- Keine sensiblen Informationen per E-Mail teilen
 - Finanzdaten, Passwörter oder vertrauliche Informationen niemals unverschlüsselt per E-Mail senden
 - Wenn notwendig, verschlüsselte Dateianhänge oder sichere Plattformen verwenden
- Verifizierung von Absendern
 - Absenderadressen sorgfältig prüfen
 - Bei unerwarteten oder verdächtigen Anfragen den Absender über eine bekannte Telefonnummer oder E-Mail kontaktieren

3. Praktischer Umgang mit Sicherheitsrichtlinien

Internetsicherheit

- **Vorsicht beim Öffnen unbekannter Webseiten**
 - Links in E-Mails oder Pop-ups meiden, wenn deren Herkunft unklar ist
 - URL-Adressen vor dem Anklicken überprüfen (z.B. durch Mouseover)
- **Nutzung von verschlüsselter Kommunikation**
 - Sicherstellen, dass Webseiten HTTPS verwenden, insbesondere bei der Eingabe von Anmeldedaten
 - Nutzung eines VPNs für sicheren Internetzugriff, insbesondere bei öffentlichen WLANs

3. Praktischer Umgang mit Sicherheitsrichtlinien

Gerätesicherheit

- Umgang mit USB-Sticks und externen Geräten
 - Nur Geräte aus vertrauenswürdigen Quellen (Originalverpackt) verwenden
 - Externe Geräte vor dem Gebrauch mit Antiviren-Software scannen
- Sperren von Computern bei Abwesenheit
 - Bildschirmsperre aktivieren, wenn der Arbeitsplatz verlassen wird
 - Verwendung von automatischen Sperrmechanismen nach Inaktivität

3. Praktischer Umgang mit Sicherheitsrichtlinien

Datenschutz

- Sicheres Speichern und Teilen von Daten
 - Daten auf geschützten Netzlaufwerken oder verschlüsselten Festplatten speichern
 - Sensible Informationen nur mit berechtigten Personen teilen
- DSGVO-Konformität beachten
 - Einhaltung der Datenschutzbestimmungen bei der Verarbeitung von Kundendaten

4. Interaktive Praxisübungen

Pishing-Quiz

- Analyse von Beispielen

Bestätigungshinweis 03-06-2020

Allgemeiner Betreff



Vodafone-team <emurueta@clientes.euskaltel.es>

Mi, 03.06.2020 14:25

An: service@mail.de

Absender



Ihr Vodafone-Team

Lieber Vodafone-Kunde,

Sie bekommen mit dieser E-Mail wichtige Informationen zu Ihrem

Vergessen Sie nicht, Ihre notwendigen Informationen zu aktualisieren, um Ihre Situationen zu regulieren. Weitere Informationen finden Sie unten:

<https://www.vodafone.de/meinvodafone>

Inhalt

Freundliche Grüße

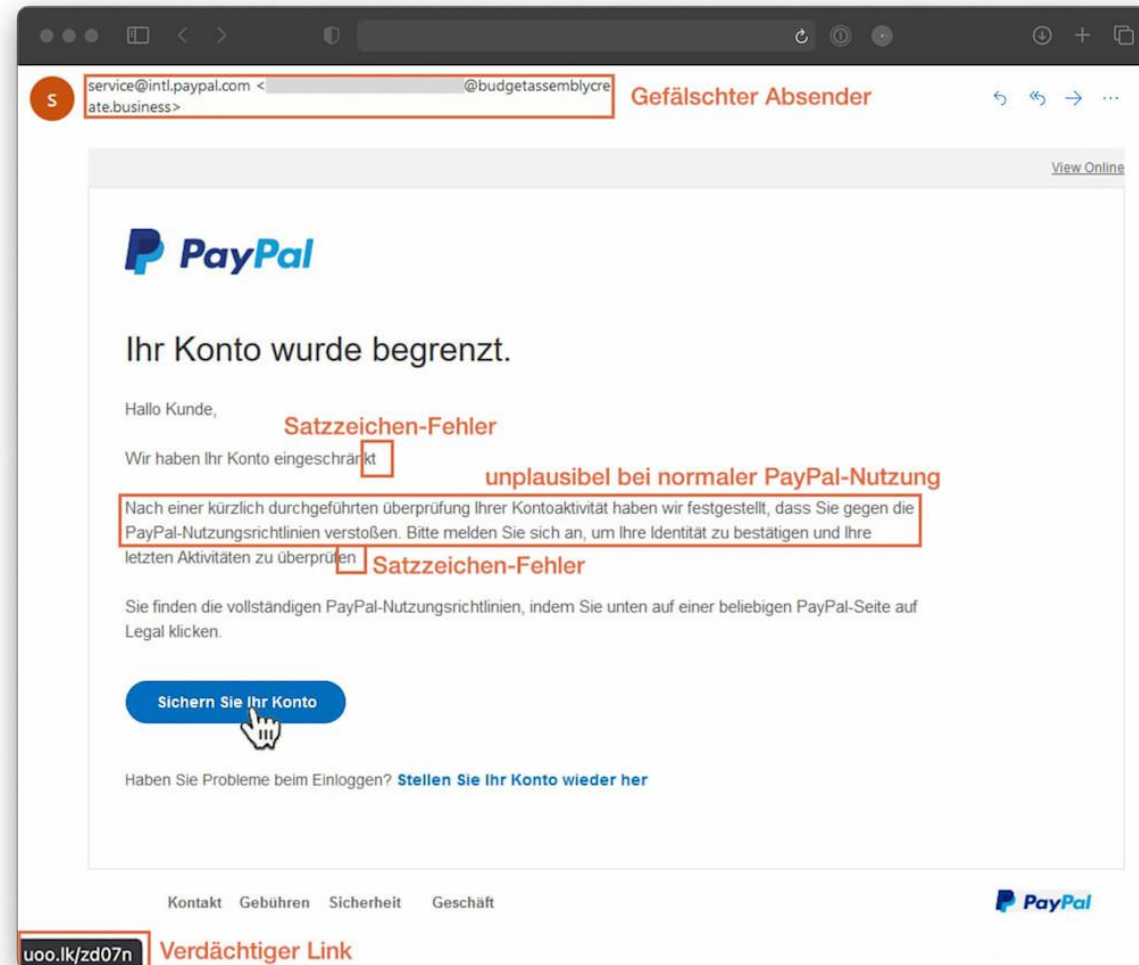
Ihr Vodafone-Team

Diese E-Mail wurde automatisch an Sie verschickt. Klicken Sie bitte nicht auf "Antworten" oder "Reply" in Ihrem E-Mail-Programm!

Sicherheitshinweis

fehlendes
Impressum





From Account Payable <post@remitrum.co>   Reply  Reply All  Forward  Archive  Junk  Delete **More** 
To  
Subject **Account Payable shared a folder with you** 1/11/22, 14:03



 October salary payment approval list by the Board Of Directors. Please review and keep for your records.

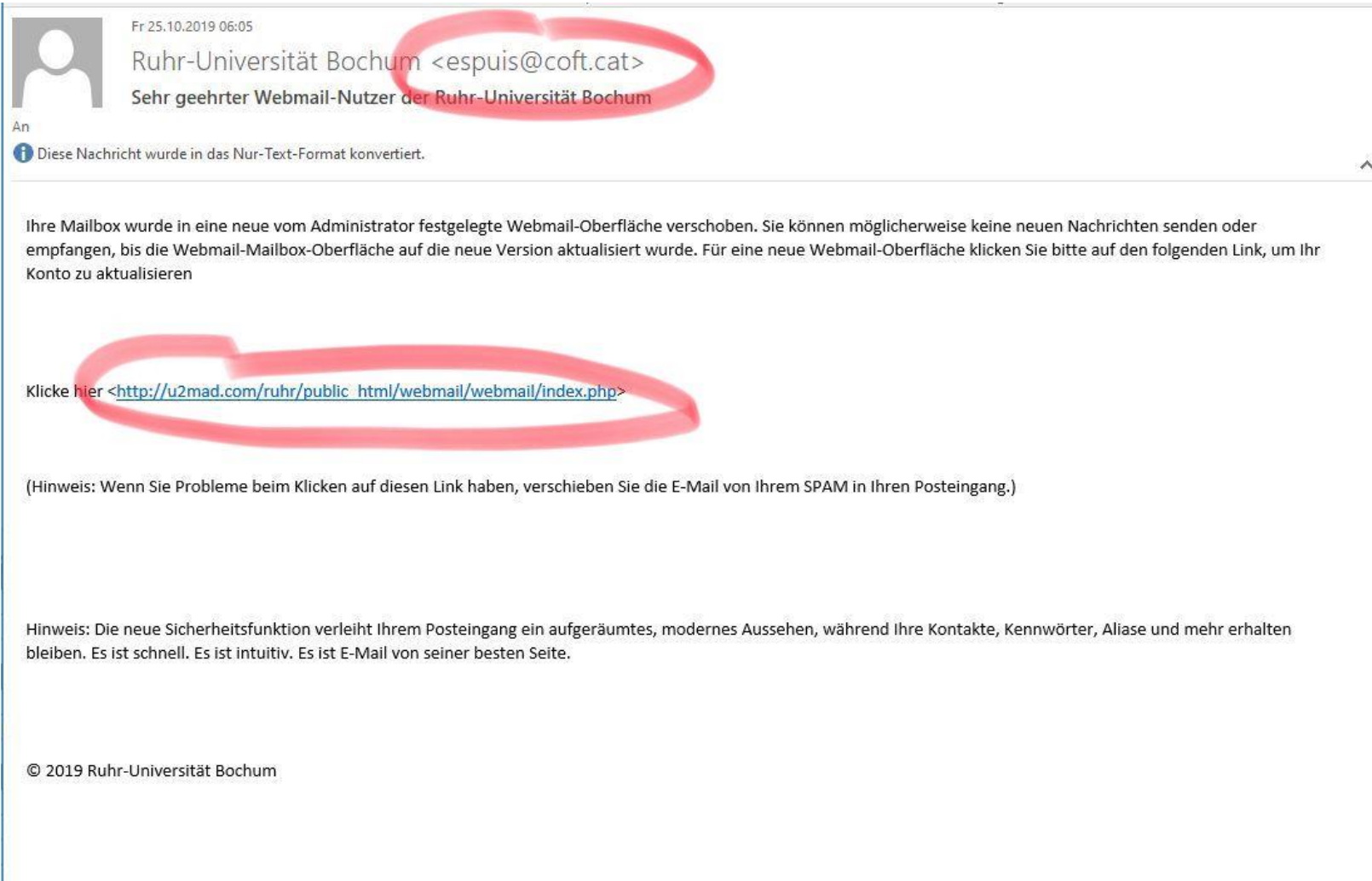


Board Approved_payroll



 Server.

[Open Contract Here](#)



Respond

Quick Steps

Move

Tags

Find

Search Junk E-Mail (Ctrl+E)

Current Folder

All Unread

By Date Newest

Last Week

Swiss Post

[SPAM] [SUSPICIOUS MAIL: ...]

Fr. 04.09

Reply

Reply All

Forward

Fr. 04.09.2020 13:09

Swiss Post <info@hipocket.co.jp>

1

[SPAM] [SUSPICIOUS MAIL: Phish]

[SPAM] Problem mit Ihrer Zustelladresse

To

Retention Policy Junk E-Mail (60 days)

Expires 03.11.2020

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.

We removed extra line breaks from this message.

We converted this message into plain text format.

Sehr geehrter Kunde,

2

Wir konnten RX572211802CH aufgrund falscher Informationen nicht zustellen.

Wir benötigen Ihre Angaben, um eine erneute Zustellung dieses Pakets zu versuchen.

Wir versuchten die Zustellung dieses Pakets am 03.09.2020 aber die angegebene Adresse war falsch, und das Paket wurde an der Tür zurückgewiesen.

Aufgrund dieser Ablehnung wurde Ihr Paket in unser Lager gebracht und wird dort noch zwei Tage bleiben, bevor es zurückgesandt wird. Sie können eine der folgenden Möglichkeiten wählen:

>> Geben Sie eine vollständige Adresse für das Paket zur erneuten

>> Zustellung an <<https://laughterfoundationcathedral.org/gorgo/>>

3

>> (zusätzliche Gebühren fallen an) Vereinbaren Sie die Zustellung des Pakets an eine alternative Adresse <<https://laughterfoundationcathedral.org/gorgo/>> (zusätzliche Gebühren fallen an) Holen Sie das Paket in unserem Lager in Belpstrasse 48, 3007 ab.

Helfen Sie uns, Ihr Paket effektiver und effizienter zuzustellen.

Vielen Dank im Voraus für Ihre Hilfe in dieser Angelegenheit und das Vertrauen in Die Post.

Mit freundlichen Grüßen,

Die Post AG



Sehr geehrte Kundin, sehr geehrter Kunde,

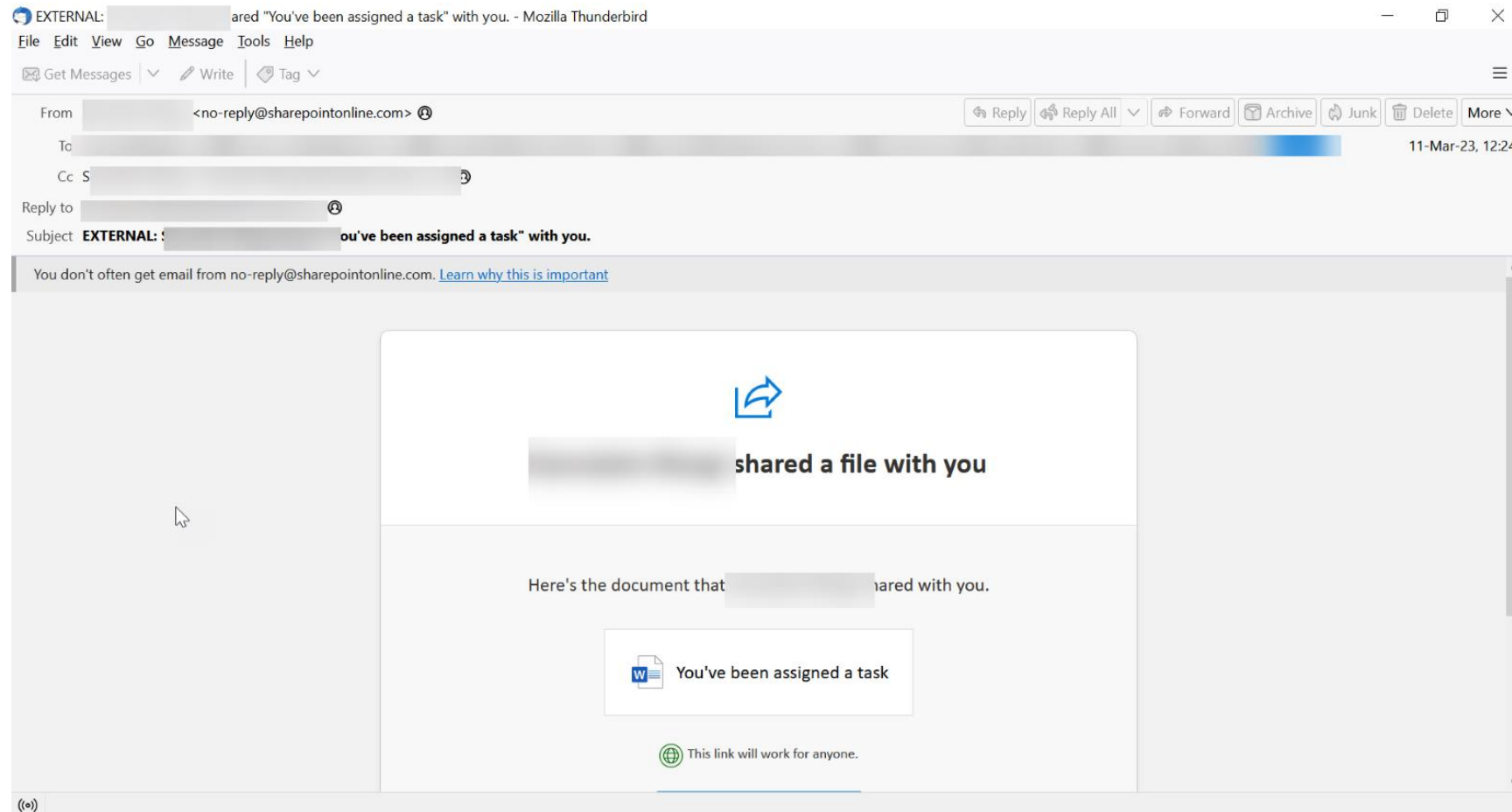
aufgrund geänderter Nutzungsbedingungen steht eine Aktualisierung Ihrer Daten an. Diese Maßnahme ist aus Sicherheitsgründen zwingend erforderlich.

Klicken Sie dafür auf den unten stehenden Button und befolgen Sie die notwendigen Schritte. Geben Sie dabei Ihre Daten vollständig und korrekt an.

Weiter zu PayPal

Mit freundlichen Grüßen,
Ihr PayPal Kundenservice





4. Interaktive Praxisübungen

Erstellen sicherer Passwörter

- Workshop

5. Abschluss und Q&A

Zusammenfassung Schlüsselpunkte

- **Starkes Passwort-Management**
 - Verwendung einzigartiger, sicherer Passwörter für jeden Account, idealerweise mit einem Passwort-Manager
- **Wachsamkeit bei E-Mails und Links**
 - Erkennen von Pishing-Versuchen, kein Klicken auf verdächtige Links oder Anhänge
- **Regelmässige Updates und Sicherungen**
 - Installieren von Sicherheitsupdates und regelmässige Backups wichtiger Daten
- **Verantwortung jedes Einzelnen**
 - Jeder trägt dazu bei, die Sicherheit der Organisation zu gewährleisten, indem aufmerksam und informiert gehandelt wird

5. Abschluss und Q&A

Fragerunde

- Offene Fragen
 - Gelegenheit, individuelle Anliegen oder spezifische Szenarien zu besprechen
- Fallbeispiele
- Weitere Schulung und Test ab 17. Februar 2025 im Selbststudium
- Interne Kontaktperson
 - Marc Schneider