

Threat Awareness

Sie fahren wie jeden Morgen zur Arbeit und schauen zuallererst in Ihr E-Mail Programm. Dabei bemerken Sie, dass Sie eine neue Nachricht in Ihrem Postfach erhalten haben.

Bei welcher der folgenden **möglichen E-Mails** gehen Sie am ehesten davon aus, dass ein **Cyberangriff** vorliegt?

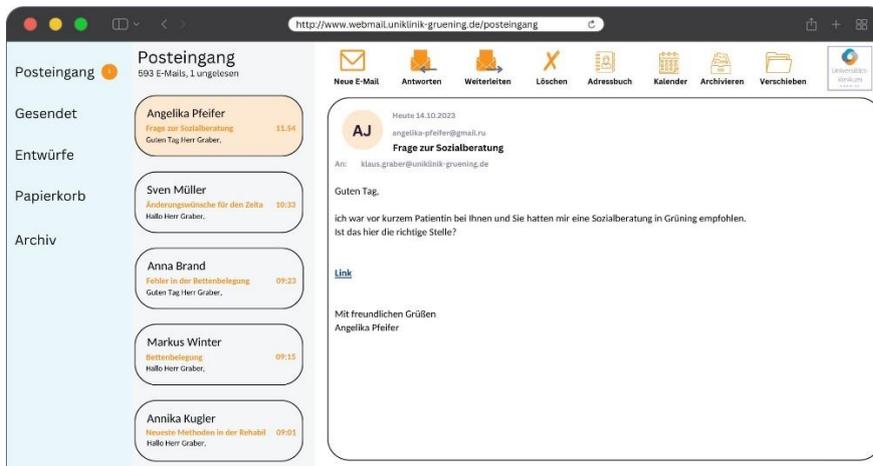
Sortieren Sie nach folgendem Schema:

[1] Ich gehe **am ehesten** davon aus, dass ein Cyberangriff vorliegt.

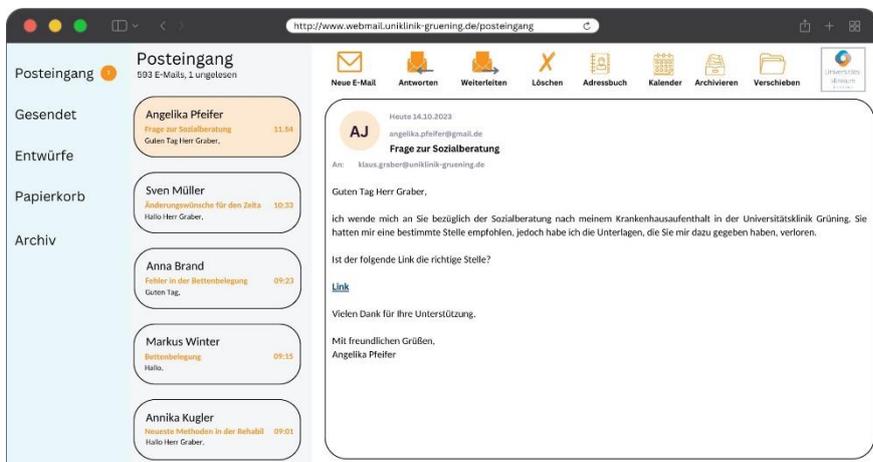
[2] Ich gehe **weniger** davon aus, dass ein Cyberangriff vorliegt.

[3] Ich gehe **nicht** davon aus, dass ein Cyberangriff vorliegt.

Impuls 1: [P 3.1.2_TA_1]



Impuls 2: [P 3.1.2_TA_2]



Impuls 3: [P 3.1.2_TA_3]

The screenshot shows a webmail interface for 'Posteingang' (Inbox) at 'http://www.webmail.uniklinik-gruening.de/posteingang'. The interface includes a left sidebar with navigation options: 'Posteingang' (593 E-Mails, 1 ungelesen), 'Gesendet', 'Entwürfe', 'Papierkorb', and 'Archiv'. The main area displays a list of emails and a detailed view of the selected one.

Posteingang
593 E-Mails, 1 ungelesen

Neue E-Mail | **Antworten** | **Weiterleiten** | **Löschen** | **Adressbuch** | **Kalender** | **Archivieren** | **Verschieben** | **UNIKLINIK GRÜNING**

Gesendet

Entwürfe

Papierkorb

Archiv

Angelika Pfeifer
Frage zur Sozialberatung 11:54
Guten Tag Herr Graber.

Sven Müller
Änderungswünsche für den Zelta 10:53
Hallo Herr Graber.

Anna Brand
Fehler in der Bettenbelegung 09:23
Guten Tag.

Markus Winter
Bettenbelegung 09:15
Hallo.

Annika Kugler
Neueste Methoden in der Rehabil 09:01
Hallo Herr Graber.

AJ Heute 14.10.2023
angelika.pfeifer@gmail.de
Frage zur Sozialberatung
An: klaus.graber@uniklinik-gruening.de

Guten Tag Herr Graber,

ich wende mich an Sie bezüglich der Sozialberatung nach meinem Krankenhausaufenthalt in der Universitätsklinik Grüning. Sie hatten mir eine bestimmte Stelle empfohlen, jedoch habe ich die Unterlagen, die Sie mir dazu gegeben haben, verloren.

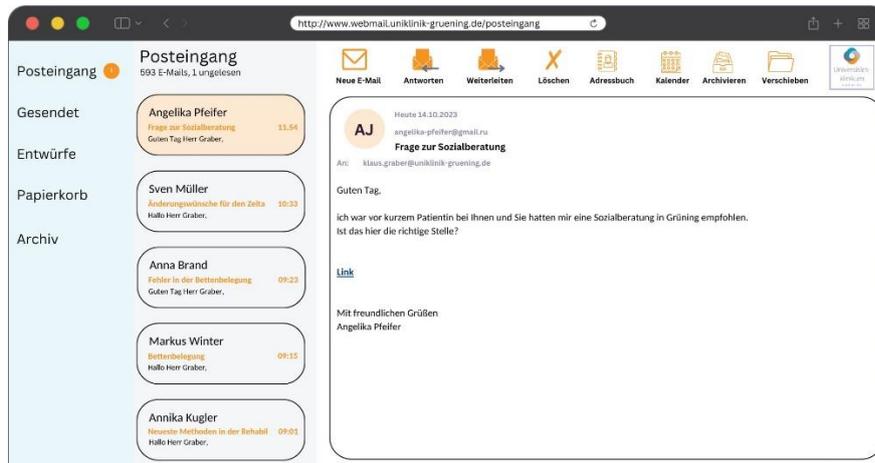
Könnten Sie mir die Unterlagen noch einmal zukommen lassen?

Vielen Dank für Ihre Unterstützung.

Mit freundlichen Grüßen,
Angelika Pfeifer

Threat Identification

Betrachten Sie bitte nochmals diese Situation:



Was konkret macht diese Nachricht zu einer **Bedrohung für die Informationssicherheit**?

Wählen Sie **zwei** Antworten aus.

- Der Absender vermittelt ein Gefühl der Dringlichkeit.
- Es handelt sich um eine private ausländische E-Mail-Adresse.
- Die E-Mail enthält Fehler in der Grammatik und Rechtschreibung.
- Die E-Mail enthält einen Link zu einer unseriösen Homepage.
- Die E-Mail ist ungewöhnlich kurz.

Threat Impact Assessment

Diese Nachricht könnte einen Cyberangriff darstellen.

Welche **Konsequenzen** könnte ein Fehlverhalten **schlimmstenfalls** für die Universitätsklinik Gröning nach sich ziehen?

Wählen Sie **zwei** Antworten aus.

Cyberkriminelle könnten ...

- Zugang zu den Informationssystemen der Universitätsklinik erhalten und sensible Daten stehlen.
- Zugang zu den Informationssystemen der Universitätsklinik erhalten, wodurch eine physische Gefährdung der Personalsachbearbeiterin eintritt.
- die medizinische Versorgung einschränken oder ausfallen lassen, so dass lebensrettende Maßnahmen verzögert oder ganz unterbrochen werden müssen.
- die Cybersecurity-Maßnahmen der Universitätsklinik erheblich überlasten, was zu Sicherheitslücken und Schwachstellen führt.
- versuchen, die Mitarbeiter:innen Zufriedenheit zu beeinträchtigen, indem sie interne Konflikte oder Missverständnisse schüren.

Tactic Choice

Welche der aufgeführten **Maßnahme** sollten Sie angesichts dieser Bedrohung als Erstes ergreifen?

Wählen Sie **eine** Antwort aus.

Ich melde die E-Mail dem/der Informationssicherheitsbeauftragten der Universitätsklinik.

Ich lösche die E-Mail und aktualisiere mein E-Mail-Postfach.

Ich hole mir schnellstmöglich eine zweite Meinung von meinen Kolleg:innen ein.

Ich überprüfe die Echtheit der E-Mail und Identität des Absenders.

Tactic Justification

Warum ist es wichtig, die Identität und die Autorisation des Absenders zu überprüfen?

Wählen Sie **eine** Antwort aus.

Um zu prüfen, ob die erhaltenen Informationen tatsächlich von einer ehemaligen Patientin stammen.

Um der Patientin schnellstmöglich eine Antwort geben zu können.

Es besteht kein Bedarf, die Echtheit der E-Mail und Identität des Absenders zu überprüfen, da das interne Netzwerk bereits ausreichend geschützt ist.

Um zu prüfen, ob die E-Mail gültig und frei verfügbar ist.

Um Zeit zu sparen und die Kommunikation effizienter zu gestalten.

Tactic Mastery

Wie geht man konkret vor, um die Echtheit der Nachricht und die Identität des Absenders zu überprüfen?

Wählen Sie **eine** Antwort aus.

- Ich achte auf das Vorhandensein einer digitalen Signatur in der E-Mail.
- Ich klicke auf den Link um zu überprüfen, ob man auf eine bössartige Website gelangt.
- Ich kontaktiere die Patientin über einen anderen Weg als die angegebene E-Mail-Adresse.
- Ich recherchiere im Internet nach der Absenderin.

Tactic Check & FollowUp

Es hat sich ergeben, dass diese E-Mail einen Cyberangriff darstellt.

Welche **ergänzende Maßnahme** zur Gefahrenabwehr ist sinnvoll oder gar notwendig?

Wählen Sie die **wichtigste** Antwort aus.

Ich lösche die E-Mail, um sie nicht ausversehen nochmal zu öffnen.

Ich leite die E-Mail meinen Kolleg:innen weiter, um sie über die Phishing E-Mail und entsprechendes Verhalten zu informieren.

Ich melde den Vorfall dem/der Informationssicherheitsbeauftragten, damit andere Mitarbeitende über den Cyberangriff und entsprechendes Verhalten informiert werden.

Ich blockiere die E-Mail-Adresse, um von ihr keine weiteren Nachrichten mehr zu bekommen.

Ich lasse mir vom E-Mail Programm automatische Umleitungen über Links blockieren.