Threat Awareness

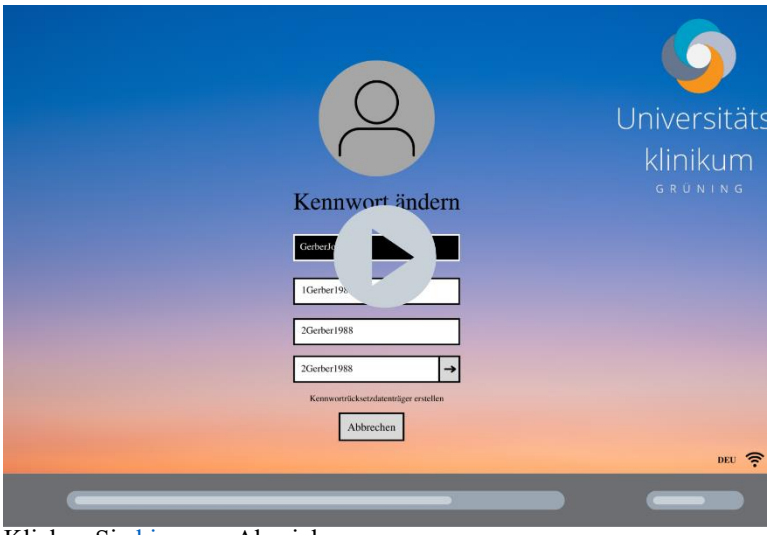
An Ihrem ersten Arbeitstag nach Ihrem Sommerurlaub möchten Sie sich am PC anmelden und werden aufgefordert Ihr Passwort zu ändern.

Welche der folgenden **möglichen Situationen** ist die **größte Bedrohung** für die **Informationssicherheit** der Universitätsklinik Grüning?

Sortieren Sie nach folgendem Schema:

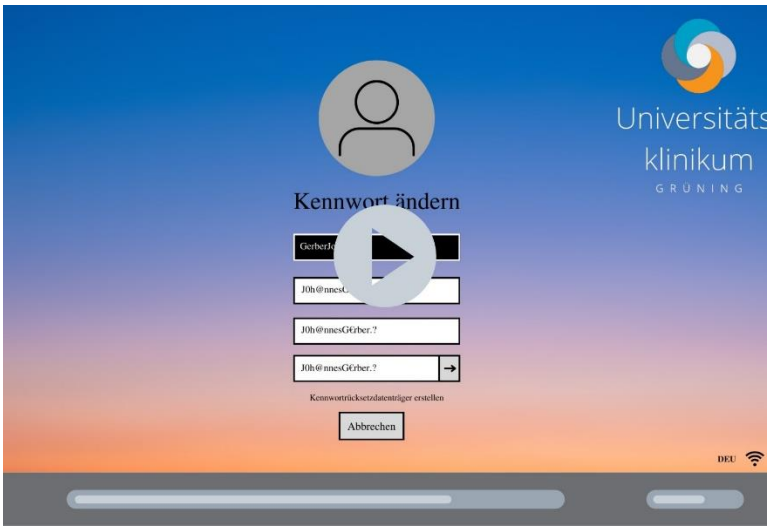
[1] Die Situation ist **am** bedrohlichsten.
[2] Die Situation ist **weniger** bedrohlich.
[3] Die Situation ist **am wenigsten** bedrohlich.

Impuls 1:



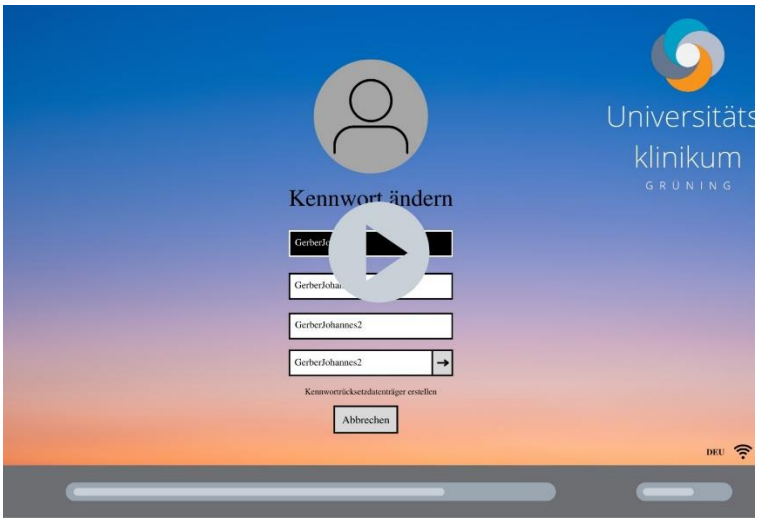
Klicken Sie hier zum Abspielen.

Impuls 2:



Klicken Sie hier zum Abspielen.

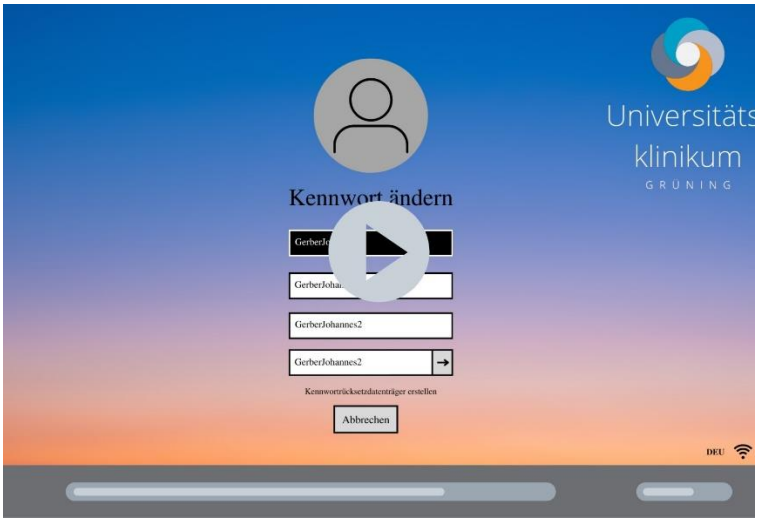
Impuls 3:



Klicken Sie hier zum Abspielen.

Threat Identification

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



Klicken Sie hier zum Abspielen.

Wählen Sie **eine** Antwort aus.

O Das Passwort enthält persönliche Daten, die mit mir in Zusammenhang gebracht werden können.

O Das Passwort kann durch den Kennwortrücksetzdatenträger von Cyberkriminellen wiederhergestellt werden.

O Das Passwort ist leicht durch sog. Wörterbuchangriffe zu entschlüsseln.

O Das Passwort enthält Kombinationen aus Tasten, die auf der Tastatur nebeneinander liegen.

O Die Benutzerkennung enthält persönliche Daten, die mit mir in Zusammenhang gebracht werden können.

Threat Impact Assessment

Welche **Konsequenzen** könnte die Wahl dieses Passworts **schlimmstenfalls** für die Universitätsklinik Grüning nach sich ziehen?

Wählen Sie **zwei** Antworten aus.

Personen könnten Ihr Passwort erraten, und …

☐ auf Gesundheitsdaten zugreifen, was eine Verletzung des Datenschutzes darstellt.

☐ könnten auf kritische Systeme zugreifen und die Patient:innenversorgung beeinträchtigen.

☐ Ihr Konto missbrauchen, um beleidigende oder unangemessene Inhalte zu verbreiten.

☐ eine Zwei-Faktor-Authentisierung installieren.

☐ physische und elektronische Sicherheitsmechanismen in der Uniklinik Grüning umgehen.

Tactic Choice

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

Wählen Sie **eine** Antwort aus.

O Keine der Antwortoptionen ist richtig.

O Ich frage meine:n Vorgesetzte:n nach einem sicheren einzigartigen Passwort.

O Ich frage den/die IT-Sicherheitsbeauftrage:n nach einem sicheren einzigartigen Passwort.

O Ich verwende dasselbe sichere Passwort das ich auch privat nutze.

O Ich verwende dasselbe sichere Passwort wie in meinen anderen Arbeitskonten auch.

Tactic Justification

Warum ist es wichtig, ein sicheres Passwort zu haben?

Wählen Sie **zwei** Antworten aus.

▢ Es trägt zur Vertraulichkeit bei, da es unbefugten Zugriff auf persönliche und sensible Daten verhindert.

▢ Es gewährleistet die Integrität von Daten, da es das Risiko von Datenmanipulation und -verfälschung minimiert.

▢ Es trägt zur Vertraulichkeit bei, da sichere und einzigartige Passwörter an Arbeitskolleg:innen weitergegeben werden können.

▢ Es trägt zur Vertraulichkeit bei, da sichere und einzigartige Passwörter an Arbeitskolleg:innen weitergegeben werden können.

▢ Es trägt zur Verfügbarkeit bei, da jederzeit die Möglichkeit besteht, das Passwort wieder zurückzusetzen.

Tactic Mastery

Wie geht man bei der Wahl eines sicheren Passworts konkret vor?

Wählen Sie **zwei** Antworten aus.

▢ Ich verwende ein 8 bis 12 Zeichen langes Passwort, das mindestens vier verschiedene Zeichenarten enthält.

▢ Ich verwende ein Passwort, das 20 bis 25 Zeichen lang ist und mindestens zwei verschiedene Zeichenarten enthält.

▢ Ich verwende ein Passwort, das 20 bis 25 Zeichen lang ist und aus einer einzigen Zeichenart besteht.

▢ Ich verwende ein 8 Zeichen langes Passwort, das nur Buchstaben und Zahlen enthält.

▢ Ich verwende ein Passwort, das 12 Zeichen lang ist und nur aus Zahlen besteht.

Tactic Check & FollowUp

Welche **ergänzenden Maßnahmen** zur Gefahrenabwehr sind in dieser Situation sinnvoll oder gar notwendig?

Wählen Sie die **zwei** Antworten aus.

☐ Ich merke mir das Passwort durch sog. Passwortmerkstrategien.

☐ Ich nutze für die Speicherung meiner Passwörter einen Passwortmanager.

☐ Ich gebe meine Arbeitspasswörter an meine Kolleg:innen weiter.

☐ Ich gebe meine Arbeitspasswörter den IT-Sicherheitsbeauftragten.

☐ Ich speichere das Passwort auf meinem Smartphone in den Notizen.

☐ Ich schreibe mir das Passwort auf einen Post-It und bewahre es unter der Tastatur auf.