

## ITS-Nudging (Trainings- und Alltags-Nudges)

im Verbundprojekt KISK: Kompetenzorientierte und  
stellenspezifische IT-Sicherheit für Mitarbeiter:innen  
in Krankenhäusern

Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages



# Komplementärer Einsatz von ITS-Nudges

## ITS-Nudging



### Trainings

Adressiert Kompetenzaufbau /  
Teilnahme an Trainings

### Arbeitsalltag

Adressiert situatives  
Bewusstsein  
komplementär zu  
Kompetenzaufbau

Der Begriff „Nudging“ wird in der Literatur unterschiedlich ausgelegt und kontrovers diskutiert [z.B. 1, 2, 3, 4].

Wir verwenden nachfolgend die Begriffe Trainings-Nudges bzw. Alltags-Nudges für *sämtliche* Materialien und Werkzeuge, die den links aufgeführten Zwecken dienlich sind.

[1]: Thaler (2018); [2]: Grüne-Yanoff & Hertwig (2016); [3]: Calo (2013); [4]: Gigerenzer (2015)

# Rekrutierungs-E-Mail zu den ITS-Trainings und/oder Kompetenzmessungen

Zur Einladung der Belegschaft zu den Trainingsinterventionen und den Kompetenzmessungen wurde folgender E-Mail-Text entwickelt.

## Theoretische Überlegungen:

Framing 1: Die Kompetenzmessungen werden als "Quiz" bezeichnet. Hiermit wird eine intrinsische Motivation gefördert, sich selbst testen zu wollen.

Framing 2: Durch die Betonung, dass die eigene Person zu IT-Sicherheit beitragen kann, und die Expertise jede:r Person wichtig (Betreff und 1. Absatz), wird die Selbstwirksamkeit der Person angesprochen.

Framing 3: Es wird der Nutzen für die eigene Person und das Krankenhaus hervorgehoben.

**Betreff: Einladung zu unserem E-Learning Kurs zur IT-Sicherheit!**

Liebe Belegschaft,

in unserer schnelllebigen, digitalen Welt spielt die Informationssicherheit eine immer wichtigere Rolle, insbesondere in sensiblen Bereichen wie dem Gesundheitswesen. Unsere Patient:innen vertrauen darauf, dass ihre persönlichen und medizinischen Daten sicher und geschützt sind. Als Mitarbeiter:innen tragen wir eine große Verantwortung, dieses Vertrauen zu wahren.

Um unser Sicherheitsniveau kontinuierlich zu verbessern, haben wir für Sie einen E-Learning Kurs zum Thema Informationssicherheit im Krankenhaus erstellt. Und hier kommen Sie ins Spiel!

Der Kurs besteht aus mehreren Modulen, in denen Sie jeweils Erklärvideos und spannende Quizzes erwarten. Diese helfen Ihnen, Ihre Kompetenzen in der Informationssicherheit Schritt für Schritt zu vertiefen.

Die Teilnahme pro Modul nimmt etwa 15 Minuten Ihrer Zeit in Anspruch.

Zur Teilnahme folgen Sie bitte folgendem Link: [Link zu den Trainings und/oder Fragebogen einfügen]

Wir hoffen auf eine rege Teilnahme und danken Ihnen im Voraus für Ihr Engagement und Ihre Unterstützung.

Bei Rückfragen melden Sie sich gerne bei mir.

Mit freundlichen Grüßen

[Ihr Name]

Abteilung Informationssicherheit

# Rekrutierungs-Poster zu den ITS-Trainings und/oder Kompetenzmessungen

Zur Einladung der Belegschaft zu den Trainingsinterventionen und den Kompetenzmessungen wurden folgende unterstützende Poster entwickelt.

## Theoretische Überlegungen:

Framing: Die Kompetenzmessungen werden als "Quiz" bezeichnet. Durch diese Darstellung wird eine spielerische und herausfordernde Atmosphäre geschaffen, die eine intrinsische Motivation der Teilnehmenden fördern soll. Indem die Teilnehmenden das Gefühl haben, ein Quiz zu absolvieren, könnten sie sich stärker engagieren und motivierter sein, ihr Wissen zu testen und zu erweitern, als wenn es einfach nur als formale Kompetenzmessung präsentiert würde.



# Trainings-Nudge: Kompetenzaufbau, Motivation und Engagement erhöhen

Zur Unterstützung der ITS-Trainings wurden ITS-Nudges entwickelt und evaluiert, die den Kompetenzaufbau unterstützen. Der „Other-orientation“ Nudge wurde in allen Trainingsvideos implementiert.

## „Other-orientation“:

**Es ist wichtig, dass du deine Patienten und Patientinnen schützen kannst.**

**Die Inhalte aus diesem Training werden dir dabei helfen, Kompetenzen aufzubauen, um deine Patienten und Patientinnen zu schützen.**

## „Self-orientation“:

**Es ist wichtig, dass du dich schützen kannst.**

**Die Inhalte aus diesem Video werden dir dabei helfen, Kompetenzen aufzubauen, um dich und deine Privatsphäre zu schützen.**

## Theorie:

Framing Social Orientation: Eine „Self-Orientation“ betont den Vorteil des Trainings für den Lernenden, wohingegen eine „Other-Orientation“ den Vorteil für die Patient:innen (z.B. höhere Resilienz) hervorhebt [1]. Die Wirkung dieser Art von Nudging basiert auf dem Kontext. Beim Einwerben von Spenden z. B. sind „Self-orientation“-Nudges effektiver [2] und egoistische Motive ein höherer Treiber als altruistische Motive.

## Implikationen:

Der „Other-Orientation“-Nudge sorgt für höheres Engagement ( $t(41) = 2.3966, p < 0.05$ ) und höhere Motivation ( $t(41) = 1.7519, p < 0.1$ ) bei der Teilnahme an ITS-Trainings. Ein Framing der Vorteile als „Self-Orientation“ hingegen sorgt für eine weniger Motivation und Engagement als in der Kontrollgruppe.

Diese Beobachtung war nicht eindeutig aus der Literatur herzuleiten, aber kann durch eine hohe Patienten-Orientierung im Gesundheitskontext erklärt werden.

# Alltags-Nudges für In-Role und Extra-Role-Verhalten

Die Alltags-Nudges teilen sich in zwei Kategorien auf. Die Alltags-Nudges adressieren entweder konkrete Verstöße („In-Role“) oder den Aufbau einer Unternehmenskultur, die durch pro-soziales Verhalten („Extra-Role“) geprägt sein soll.

## Alltags-Nudges



In-Role- und Extra-Role-Verhalten sind zwei unterschiedliche Arten von Sicherheitsverhalten [1].

Unter In-Role-Verhalten versteht man das Befolgen von expliziten Regeln und Vorschriften als Bestandteil des Jobs [2]. Beispiele sind die Nichtweitergabe von Passwörtern, das Sperren von PCs oder einfach gesagt: die Einhaltung der geltenden Vorschriften. In-Role-Verhalten hängen in erster Linie von den Kompetenzen des Einzelnen ab.

Extra-Role-Verhalten sind nicht über Vorschriften geregelt und das Nichtbefolgen dieser Verhalten kann auch nicht bestraft werden [2]. Beispiele für diese Art von Verhalten sind: das Helfen Anderer, freiwilliges Weitergeben von (ITS)-Wissen oder andere zu erinnern, sich vom PC abzumelden. Extra-Role-Verhalten sind gekennzeichnet durch Freiwilligkeit einerseits und Veranlagung andererseits. Die Motivation ist eine intrinsische.

[1]: Hsu et al. (2015); [2]: Davis et al. (2021)

# Der SchutzFuchs als Repräsentant für Informationssicherheit

Der Fuchs wird der Botschafter für IT-Sicherheit.

## 1. In-Role

Der Fuchs wird langfristig von der Belegschaft mit ITS assoziiert. Wenn der SchutzFuchs an risikobehafteten Orten platziert wird, wird diese Assoziation genutzt, um situatives Bewusstsein zu schaffen. Ein bekanntes Beispiel ist der “Watching-Eye-Effekt”, der nachweislich sowohl prosoziales Verhalten fördert, als auch im situativen Nudging an ITS erinnern kann.

## 2. Extra-Role

Besonderes pro-soziales ITS-Verhalten wird durch Schenkung des Maskottchens belohnt und anerkannt. Hierfür können Wettbewerbe und Gewinnspiele etabliert werden. So wird eine extrinsische Motivation gefördert.



# Förderung pro-sozialer ITS-Verhalten durch extrinsische Motivation

## Extra-Role

Besonderes pro-soziales ITS-Verhalten wird durch Schenkung des Maskottchens belohnt und anerkannt. So soll eine Kultur um ITS im Krankenhaus aufgebaut und gefördert werden.

Der Repräsentant für ITS, der “Schutzfuchs” in Form eines Plüschfuchses ist eine **Initiative zur Motivation zu prosozialen (freiwilligen) organisationalen Informationssicherheitsverhalten.**

Durch die Verschenkung des Maskottchens an Mitarbeiter:innen mit besonderen prosozialen Verhalten (z.B. Meldung von auffälligen E-Mails) wird **eine extrinsische Motivation geschaffen, die selbstbestimmt und stark internalisiert ist** (“Internal PLOC”, [1][2]).

Hiermit schafft diese Verhaltensintervention durch den Belohnungsanreiz **Awareness und eine Unternehmenskultur gekennzeichnet durch prosoziales Engagement** gleichermaßen.



[1]: Ryan & Connell (1989); [2]: Malhotra et al. (2008)

# Clean Desk

In-Role

Verwaltungsfachpersonal

## Problem:

Liegenlassen sensibler Dokumente auf Schreibtischen, sodass Unbefugte Auspähen können

## Lösung:

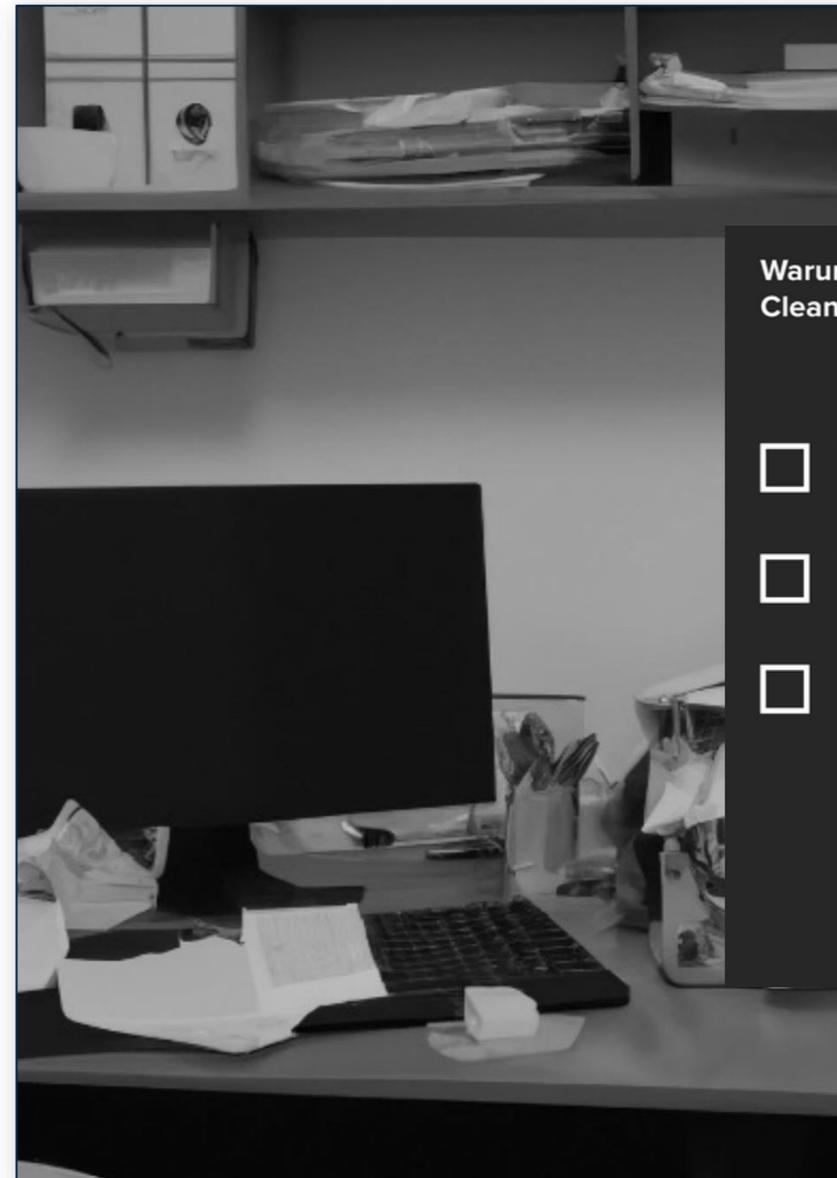
Informationskarten, die auf Schreibtischen verteilt werden.

## Theorie:

Boost (Threat Identification, Threat Impact Assessment)

## Umsetzung, Durchführung, Aufwand:

Flyer, DIN A7, 400g; 26 €/1000 St.  
Verteilung auf Schreibtischen oder in Postfächern.



### Warum ist die Einhaltung der Clean Desk Policy wichtig?

- Ein sauberer Schreibtisch kann Stress reduzieren.
- Damit keine sensiblen Informationen in falschen Hände geraten.
- Damit man den Stift nicht ständig suchen muss.

# Clean Desk

In-Role

Verwaltungsfachpersonal

## Problem:

Liegenlassen sensibler Dokumente auf Schreibtischen, sodass Unbefugte Ausspähen können

## Lösung:

Sticker mit der Aufschrift „Können Sie mich sehen?“ und Erklärungstext klebend auf Schreibtischen, so platziert, dass sie nur bei einem aufgeräumten Schreibtisch sichtbar sind.

## Theorie:

Feedback, System 1/2 Nudge

## Umsetzung, Durchführung, Aufwand:

Sticker Indoor leicht ablösbar (9,8cm); 63 €/1000 St.

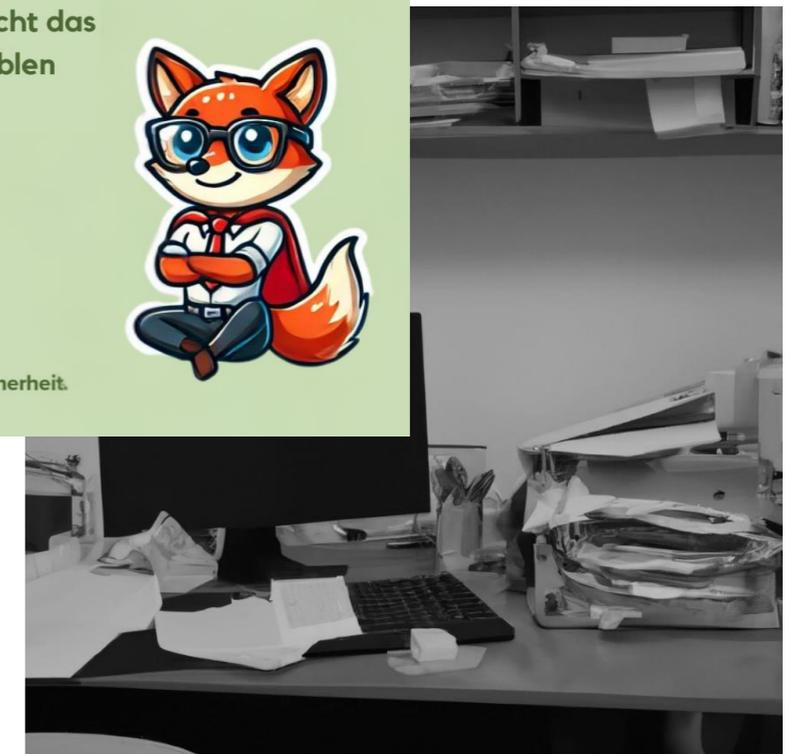
Platzierung auf Dienstschreibtischen (zur Vermeidung von Reaktanz sollte nicht unbedingt in private Arbeitsbereiche eingegriffen werden. Idealerweise einen Mitarbeiter- oder Platzwechsel abwarten.)

## Können Sie mich sehen?

Das Liegenlassen von Dokumenten ermöglicht das Ausspähen von sensiblen Daten.



Patienten- und Informationssicherheit.  
Die Verantwortung aller.



# Verschließen von Türen

In-Role

Verwaltungsfachpersonal

## Problem:

Türen werden nicht (ab)geschlossen beim Verlassen des Raumes.

## Lösung:

Sticker auf Tür und Türrahmen zeigen ein Bild oder einen Spruch, der sich durch das Schließen der Tür vervollständigt.

Ist die Tür offen, zeigt sich der Spruch „Ich bin da“. Ist die Tür geschlossen, zeigt sich der Spruch „Ich bin gleich wieder da“.

Mitarbeiter:innen werden so gleichzeitig erinnert und motiviert.

## Theorie:

Feedback, Boost, Motivation

(Belohnungseffekt durch Vervollständigung einer Aufgabe)



# Interventionszone „Wer wird Millionär“

## Interventionszone

- Durch die Platzierung der Plakate an einem stark frequentierten Bereich wie den Eingängen des Krankenhauses wird die Aufmerksamkeit der Mitarbeiter:innen unmittelbar auf die präsentierten Themen gelenkt.
  - 5 Themen (WhatsApp, Shoulder Surfing, Clean Desk, Phishing, Fotos)
  - Jedes Thema/Poster mit einem Mini-Quiz, um Engagement zu fördern
  - Als Überraschung dürfen sich die Teilnehmenden am Ende der Interventionszone z. B. ein Webcam-Sticker mitnehmen



# Interventionszone „Wer wird Millionär“

Testen Sie sich beim Security-Quiz!

Die Poster sind von links nach rechts zu betrachten. Bilden Sie ein Lösungswort aus allen Aufgaben. Als Belohnung bei richtigem Lösungswort gibt es leider keine 1 Millionen Euro zu gewinnen, sondern eine andere Überraschung.

**1.000 €**

## Zweitmeinung?

### Ja! Aber nicht über Social Media.

Private Messenger wie WhatsApp sind in der Nutzung unkompliziert, können aber schlimmstenfalls Datenverlust und Rufschädigung unseres Hauses bedeuten. Selbst wenn ein Anonymisierungsversuch getätigt wurde, kann es sein, dass eine Re-Identifikation durch weitere im Internet vorliegende Informationen möglich ist.

Da die Daten auf fremden Servern gespeichert werden, hat man keine Kontrolle darüber was damit passiert. Daher besteht ein Datenschutzverstoß, wenn ohne Zustimmung der betreffenden Person Daten an Externe weitergegeben werden. Die Vertraulichkeit der Daten wird verletzt. Zweitmeinungen sollten lieber über freigegebene Kommunikationssysteme eingeholt werden. Nur so kann der Schutz von personenbezogenen Daten gewährleistet werden.



In welchem Jahr wurde WhatsApp von Facebook übernommen?

A: 2010      B: 2012

C: 2014      D: 2016

Die richtige Lösung lautet: C



} Platz für Partner-Logo

} Threat Awareness

} Threat Impact Assessment

} Tactic Justification

# Interventionszone „Wer wird Millionär“

Testen Sie sich beim Security-Quiz!

Die Poster sind von links nach rechts zu betrachten. Bilden Sie ein Lösungswort aus allen Aufgaben. Als Belohnung bei richtigem Lösungswort gibt es leider keine 1 Millionen Euro zu gewinnen, sondern eine andere Überraschung.

**8.000 €**

## Wer schaut gerade alles zu?

Shoulder Surfing, also das unbemerkte Ausspähen durch Unbefugte, stellt ein ernstzunehmendes Sicherheitsrisiko dar. Jede Person in Ihrem Umfeld hat Zugang zu vielen persönlichen und vertraulichen Informationen. Diese Informationen sind jedoch nicht für jede Person bestimmt. Das unbemerkte Ausspähen von Informationen (Shoulder Surfing) kann zu Datenschutzverletzungen führen.

Es ist nicht immer so offensichtlich wie in diesem Bild. Sei es ein\*e neugierige\*r Patient\*in, der\*die durch die Tür des Arztzimmers Befunde oder Abrechnungen einsehen kann oder eine unbefugte Person, die in Leitstellen oder Pausenräume schießt. Durch das Vermeiden von Shoulder Surfing minimieren Sie das Risiko eines unautorisierten Zugriffs durch Dritte. So wird die Vertraulichkeit der Daten Ihrer Patient\*innen sowie Kolleg\*innen gewahrt und Sie verhindern eine Datennutzung für unsachgemäße Zwecke.

Was ist "Shoulder Surfing"?

- W: Durchsuchen von Müll
- X: Hacking
- Y: Ausspähen von Informationen
- Z: Sicheres Internet-Surfen

Die richtige Lösung lautet: Y



Platz für Partner-Logo

Threat Awareness

Threat Impact Assessment

Tactic Justification

# Interventionszone „Wer wird Millionär“

Testen Sie sich beim Security-Quiz!

Die Poster sind von links nach rechts zu betrachten. Bilden Sie ein Lösungswort aus allen Aufgaben. Als Belohnung bei richtigem Lösungswort gibt es leider keine 1 Millionen Euro zu gewinnen, sondern eine andere Überraschung.

**32.000 €**

## Arbeitsplatz aufgeräumt?

Unordentliche Schreibtische oder offen herumliegende Akten können nicht nur zu einem Verlust von wichtigen Unterlagen führen, sondern auch unbeabsichtigten Einblicken in vertrauliche Daten von Patient\*innen Vorschub leisten. Jede Person, die befugt oder unbefugt deinen Arbeitsplatz betritt, hat Zugang zu vielen persönlichen und vertraulichen Informationen. Es kann zu schwerwiegenden Datenschutzverletzungen kommen. In der falschen Hand können diese Daten zum Beispiel genutzt werden, um Personen zu erpressen, Phishing-Attacken durchzuführen oder die Informationen können verkauft werden.

Akten von Patient\*innen, Abrechnungen oder persönliche Notizen sollten nicht via Papier oder Bildschirm für unbefugte Personen sichtbar sein, da sie datenschutzrelevant sind und gezielte Cyberangriffe ermöglichen. Durch diese Maßnahmen minimieren Sie das Risiko eines unautorisierten Zugriffs durch Dritte wie zum Beispiel durch Patient\*innen oder ihre Angehörigen. Dadurch wird die Vertraulichkeit der Daten gewahrt und Sie verhindern eine Datennutzung für unsachgemäße Zwecke.

Was ist das Hauptziel einer "Clean Desk Policy"?

- A: Nachhaltigkeit fördern
- B: Sicherheit erhöhen
- C: Produktivität steigern
- D: Kosten reduzieren

Die richtige Lösung lautet: B



} Platz für Partner-Logo

} Threat Awareness

} Threat Impact Assessment

} Tactic Justification

# Interventionszone „Wer wird Millionär“

Testen Sie sich beim Security-Quiz!

Die Poster sind von links nach rechts zu betrachten. Bilden Sie ein Lösungswort aus allen Aufgaben. Als Belohnung bei richtigem Lösungswort gibt es leider keine 1 Millionen Euro zu gewinnen, sondern eine andere Überraschung.

**500.000 €**

## Klingt irgendwie seltsam?

Phishing kann besonders gravierende Folgen haben, da Gesundheitsdaten zu den sensibelsten persönlichen Informationen zählen. Datendiebstahl kann u.a. zu Reputationsverlust, zu psychologischen und finanziellen Schäden führen.

Das Ziel bei der Arbeit mit Daten von Patient\*innen ist, diese vertraulich zu behandeln und keine Informationen an unbefugte Dritte offenzulegen. Um Daten zu sammeln oder größere Hackerangriffe vorzubereiten, verwenden Cyberkriminelle häufig Phishing-Mails. Dabei geben sich Kriminelle zumeist als andere Personen aus. Durch den Einsatz von KI ist es den Cyberkriminellen jetzt auch möglich, täuschend echte Phishing-Mails zu erstellen. Daher gilt es, immer skeptisch zu sein, denn mit dem Klick auf den Link könnten Geräte mit Viren infiziert, ausspioniert oder verschlüsselt werden.

Was ist das Hauptziel von Phishing-Angriffen?

- C: Computerviren verbreiten
- D: Lizenzen überprüfen
- E: Vertrauliche Daten stehlen
- F: Internetzugang testen

Die richtige Lösung lautet: E



Platz für Partner-Logo

Threat Awareness

Threat Impact Assessment

Tactic Justification

# Interventionszone „Wer wird Millionär“

**Testen Sie sich beim Security-Quiz!**

Die Poster sind von links nach rechts zu betrachten. Bilden Sie ein Lösungswort aus allen Aufgaben. Als Belohnung bei richtigem Lösungswort gibt es leider keine 1 Millionen Euro zu gewinnen, sondern eine andere Überraschung.

**1.000.000 €**

## Selfie-Time!

Kurz vor der Mittagspause noch schnell ein Foto machen und an Freunde und Bekannte senden? Unbemerkt können sich im Hintergrund vertrauliche Informationen, wie Schichtpläne, Daten von Patient\*innen oder Befunde befinden. Diese gilt es zu schützen, denn fälschlich veröffentlichte (Patient\*innen)-Daten können zur Verletzung der Privatsphäre und zu Stigmatisierung führen.

Generell sollte beim Erstellen von Fotos oder Videos immer darauf geachtet werden, dass keine sensiblen Informationen zu sehen sind oder andere Personen dadurch Schaden erleiden. Zu sensiblen Daten zählen beispielsweise Schichtpläne, Daten von Patient\*innen, Befunde, Bewerbungen oder Abrechnungen. Denn sobald diese versendet wurden, hat man keine Kontrolle mehr darüber, was damit passiert. Die Vertraulichkeit der Daten wird somit verletzt. Dabei spielt es keine Rolle, ob diese Bilder auf Instagram gepostet werden oder an Freunde per WhatsApp gesendet werden.

Wie viele Snaps (Fotos) werden täglich über die Plattform Snapchat versendet?

Q: 400.000	R: 4.000.000.000
S: 4.000.000	T: 40.000.000

Die richtige Lösung lautet: R



**KISK**

} Platz für Partner-Logo

} Threat Awareness

} Threat Impact Assessment

} Tactic Justification

# Umgang mit sensiblen Daten am Arbeitsplatz (Clean Desk) - Aufsteller

## Mensaaufsteller

- Mensaaufsteller werden gezielt im alltäglichen Umfeld des Verwaltungsfachpersonals platziert.
- Durch ihre auffällige Platzierung auf Tischen lenken sie die Aufmerksamkeit unaufdringlich, aber wirkungsvoll auf eine bestimmte Botschaft oder Information.
- Durch die wiederholte Sichtbarkeit an einem Ort, der oft besucht wird, steigt die Wahrscheinlichkeit, dass die Botschaft wahrgenommen und verinnerlicht wird, was das Verhalten subtil beeinflussen kann.



# Umgang mit sensiblen Daten am Arbeitsplatz (Clean Desk) - Aufsteller



Platz für Partner-Logo



Threat Awareness

Threat Impact Assessment

# Umgang mit sensiblen Daten am Arbeitsplatz (Clean Desk) - Poster

## Stationsposter

- Schwarze Bretter befinden sich häufig an zentralen Punkten, wo sie von Mitarbeiter:innen regelmäßig betrachtet werden.
- Ein Poster, das dort platziert wird, profitiert von der Erwartungshaltung der Betrachter, nützliche oder notwendige Informationen zu finden. Dies erhöht die Wahrscheinlichkeit, dass die Botschaft des Posters ernst genommen und in Betracht gezogen wird.
- Da Mitarbeiter:innen regelmäßig an diesen Brettern vorbeikommen, sehen sie das Poster wahrscheinlich mehrmals.



# Umgang mit sensiblen Daten am Arbeitsplatz (Clean Desk) - Poster



} Threat Awareness

} Platz für Partner-Logo

Threat Impact Assessment

Tactic Choice & Tactic Mastery