So handeln Sie richtig

am Arbeitsplatz

ARS DOCENDI ACADEMY

Social Engineering

Vorsicht bei drängendem Ton

Personen, die unter Berufung auf ihre Autorität (Vorgesetzter etc.) oder Dringlichkeit („Die Zeit drängt…“, „Sie behindern…“) auf Informationen drängen, haben fast immer kriminelle Absichten.

Social Engineering

ARS DOCENDI ACADEMY

Jede kann Opfer eines Angriffs werden

Die Angreifer wenden sich sehr oft an Personen, die keine sicherheitsrelevanten Aufgaben haben, weil sie der Meinung sind, dass diese Personen nicht so sensibel für das Thema Datensicherheit sind.

Deren Zugang wird dann von den Angreifern als Sprungbrett genutzt, um weiter in die Systeme unseres Unternehmens einzudringen.

ARS DOCENDI ACADEMY

Social Engineering

Links mit Vorsicht anklicken

Klicken Sie auf keinen Fall auf Links, die Sie nicht kennen oder bei denen Sie unsicher sind, woher sie stammen. Es ist immer besser, die entsprechende URL manuell in den Browser einzugeben, als auf einen verdächtigen Link zu klicken.

Social Engineering

ARS DOCENDI ACADEMY

Regelmäßige Updates

Mitarbeitende sollten darauf achten, dass ihre Geräte und Software immer auf dem neuesten Stand sind. Nur so können Sicherheitslücken geschlossen werden.

Verdächtige Aktivitäten melden

Wenn Sie eine verdächtige Aktivität bemerken oder den Verdacht haben, dass Sie das Ziel eines Social-Media-Angriffs geworden sind, sollte Sie dies umgehend der IT-Abteilung melden.

Wenn Sie Zweifel haben,

- lassen Sie sich eine Rückrufnummer geben, die Sie überprüfen können.

- erkundigen Sie sich bei Vorgesetzten oder Kollegen, ob die anfragende Person vertrauenswürdig und "echt" ist.

Social Engineering

ARS DOCENDI ACADEMY

Überweisen Sie **NIE** Geldbeträge, ohne sich intern abgesichert zu haben.

Social Engineering

ARS DOCENDI ACADEMY