Erkennen von Phishing-E-Mails

Die folgende Checkliste soll dabei helfen, Phishing-E-Mails zu erkennen.

Handelt es sich um eine unerwartete E-Mail und kann eine der Fragen mit „Ja" beantwortet werden, muss achtsam vorgegangen werden und ggfs. der Systembetreuer zur Beratung herangezogen werden.

Frage	Erläuterung
1. Bestehen Zweifel an der Echtheit der E-Mail?	• Ist der Absender bekannt? • Kann der Absender den Versand telefonisch oder persönlich bestätigen?
2. Enthält die E-Mail Drohungen in Verbindung mit dringlichen Handlungsaufforderungen?	• In der E-Mail wird dringender Handlungsbedarf signalisiert. • Etwas muss sofort erledigt werden (z. B. Überweisung, Reaktivierung eines Accounts). • Wenn – dann – Szenario • Im Text wird eine Drohkulisse mit angeblichen schwerwiegenden Konsequenzen aufgebaut (z. B. Löschung des Accounts, Sperrung des Geschäftskontos).
3. Ist die Anrede unpersönlich oder untypisch?	• Ihr Name wird nicht in der Anrede verwendet. • Die Anrede oder die Abschiedsformulierung sind zu förmlich oder zu lax.
4. Sind in der E-Mail Links enthalten?	• Verlinkung zu Webseiten • Fahren Sie mit dem Mauszeiger über den Link (Mouse-over). Welche URL wird angezeigt? • Sie dürfen in keinem Fall auf Links klicken, die sich in unerwünschten und unerwarteten E-Mails befinden.
5. Müssen persönliche Informationen eingegeben werden?	• Dabei kann es sich z. B. um Passwörter oder Login-Daten handeln.
6. Weist der Nachrichtentext sprachliche und grammatikalische Unzulänglichkeiten auf?	• Umlaute werden nicht dargestellt (z. B. ae statt ä) • Der Text ist in schlechtem Deutsch verfasst. • Der Text enthält Rechtschreibfehler. • Satzzeichen werden falsch verwendet.