Wie gehe ich vor, wenn ich eine E-Mail erhalte, deren Inhalt mir nicht vertrauenswürdig erscheint?

Rechnungen, Mahnungen und Anwaltsschreiben werden mittlerweile oftmals elektronisch verschickt. Die Gründe sind einfach: schnelle und kostengünstige Zustellung, wenig Verwaltungsaufwand für die Firmen. Doch eben diese Vorteile bringen die Gefahr mit sich, dass Kriminelle E-Mails mit Forderungen verschicken.

Aus diesem Grund sollten Sie sich vor jeder E-Mail die sie Öffnen fragen, ob Sie wirklich eine solche E-Mail erwarten.

Das öffnen der E-Mail im Posteingang (**NUR** das Öffnen der **Nachricht!**) birgt in der Regel keinerlei Gefahren. Lediglich das Anklicken von Links oder Anhängen, die der Nachricht angefügt sind kann zu einer Infizierung führen!

Wir haben Ihnen hier eine kurze Checkliste zusammengestellt, mit er Sie überprüfen können, ob der Inhalt dieser E-Mail vertrauenswürdig zu sein scheint:

Kenne ich den Absender der E-Mail?

Erwarte ich eine dem Betreff entsprechende E-Mail (z.B. MAHNUNG)?

Erscheint mir der in der E-Mail genannte Absender vertrauenswürdig und nicht fiktiv (Firmenimpressum enthält Rechtsform, Adresse und Telefonnummer)?

Findet man bei Suchmaschinen wie Google Informationen über das Unternehmen (Firmenauftritt, Branchenverzeichniseinträge)?

Enthält die E-Mail Dateianhänge?

Rechtfertigt der Inhalt der E-Mail einen Dateianhang?

Erscheint mir der Dateityp des Anhangs passend zum Inhalt?

Übliche Dateiendungen für Dokumente: .pdf, .doc(x), .xls(x), .odf, .txt

Übliche Dateiendungen für Kalender/Kontakte/E-Mails: .vcf, .msg

Dateiendungen, die möglicherweise gefährlich sind: .zip, .rar, .tar.gz, .lnk, .7z

ACHTUNG! Gefährliche Dateiendungen: .exe, .bat, .cmd, .vbs, .com

Ist die Wortwahl und die Rechtschreibung der E-Mail dem Absender angemessen?

Z.B.: Ein mit Rechtschreib- und Satzstellungsfehlern gespickter Text kommt i.d.R. nicht von einer staatlichen Behörde.

Sind die Forderungen in der E-Mail realistisch?

Z.B.: Ein Kreditunternehmen würde Sie niemals nach vertraulichen Daten in einer E-Mail fragen.

Würden Sie die in der E-Mail gestellte Forderung unverschlüsselt über das Internet verschicken?

Wie verfahre ich mit der E-Mail in meinem Posteingang?

Wenn Sie nach der Prüfung nach oben genanntem Schema feststellen, dass die E-Mail vermutlich infiziert oder unseriös ist, sollten Sie die Nachricht sofort löschen. Wenn Sie nicht sicher sind und die Nachricht aus diesem Grunde noch aufbewahren möchten, sollten Sie diese in einen eigenen Ordner verschieben um sicherzustellen, dass sie nicht aus versehen geöffnet und der Anhang ausgeführt wird. Erstellen Sie sich aus diesem Grunde am Besten einen Unterordner mit einem eindeutigen Namen (z.B. „Infiziert“) in Ihrem Postfach und verschieben Sie die Nachricht in diesen. Sie sollten den Ordner in regelmäßigen Zyklen leeren.