# Sicherheits-Irrtümer: E-Mail-Sicherheit

## Irrtum 1: "Wenn ich eine E-Mail nur anschaue, aber keinen Anhang öffne, kann nichts passieren."

**Leider trifft das nicht zu.** Viele E-Mails werden heute im **HTML-Format** verschickt. Im Gegensatz zu **reinen Text-E-Mails** sind diese oftmals farbig, mit verschiedenen Schriften und Grafiken gestaltet. Im so genannten **Quellcode** einer HTML-formatierten E-Mail **lauert die Gefahr**: Denn dort kann schädlicher Code versteckt sein, der bereits beim Öffnen der HTML-E-Mail auf dem Computer des Empfängers ausgeführt wird, ohne dass dafür ein Anhang angeklickt werden muss.

## Irrtum 2: "Das Antworten auf Spam-Mails birgt keine Gefahr, man kann auch den Links zum Löschen aus dem Verteiler folgen."

**Das stimmt nicht.** Egal, um welche Art unaufgeforderter E-Mail es sich handelt, sollten Empfänger diese ignorieren und umgehend löschen, am besten ohne sie zuvor überhaupt zu öffnen. **Auf gar keinen Fall sollten Nutzer Links folgen, die vermeintlich dazu führen, dass die Empfängeradresse aus der Liste gelöscht wird.** Denn sobald Sie als Empfänger auf solch eine E-Mail reagieren, weiß der Versender, dass Ihre Adresse gültig und aktiv ist.

## Irrtum 3: "Eine E-Mail kommt immer von der Adresse, die im Absender-Feld steht."

**Das ist falsch, denn Absenderadressen von E-Mails können mit geringem Aufwand beliebig gefälscht werden.** Hinter dem in einer E-Mail angezeigten Namen einer Person oder Organisation kann sich ein ganz anderer Absender verbergen – dies ist üblicherweise bei illegalen Aktivitäten der Fall, wie Spam-Versand oder den Versuch, den Computer eines Nutzers mit Schadsoftware zu infizieren. **Einen ersten Hinweis auf den Absender** erhält der Nutzer, wenn er mit der Maus über den angezeigten Namen fährt. Je nach E-Mailprogramm wird dann neben der Maus oder am unteren Bildschirmrand die – angeblich – verwendete E-Mail-Adresse angezeigt.

**Die Echtheit des Absenders** lässt sich durch die Verifikation des so genannten E-Mail-Headers ermitteln. Der Header beziehungsweise Quelltext der E-Mail kann im E-Mail-Programm angezeigt werden. In den mit "Received From" bezeichneten Zeilen können Nutzer den Weg der Mail verfolgen, der Versender findet sich in der letzten Received From-Zeile. **Teilweise manipulieren Angreifer aber auch die Received-Zeilen**, sodass es schwieriger wird, die tatsächliche Herkunft der E-Mail festzustellen. ***Deswegen gilt bei Zweifeln an der Herkunft einer E-Mail immer: Nicht öffnen, sondern direkt löschen.***

## Irrtum 4: "Phishing-Mails sind leicht zu erkennen."

**Falsch.** Die Aufmachung solcher Mails und auch der Webseiten, auf die darin enthaltene Links führen, sehen den Original-Mails und Webseiten oftmals täuschend ähnlich. Die Versender von Phishing-Mails agieren jedoch immer professioneller, sodass auch eine korrekte Anrede oder ein plausibler Inhalt keine Gewissheit bieten.