

## Anleitung zur Weiterleitung zur Prüfung von E-Mails mit Phishing/Spam

### E-Mail als Anhang weiterleiten

E-Mails die Sie zu Phishing/Spam-Prüfungen im EML- oder MSG-Format an den LIWEST Kundenservice ([spammeldung@teamlwest.at](mailto:spammeldung@teamlwest.at)) weiterleiten, müssen vor dem Versand gepackt werden.

#### E-Mail-Programm: E-Mail in Anhang konvertieren

##### Thunderbird

1. Öffnen oder markieren Sie die E-Mail, die weitergeleitet werden soll.
2. Wählen Sie im Menü „**Nachricht** > **Weiterleiten als** > **Anhang**“. Eine neue E-Mail wird erzeugt.
3. Tragen Sie den neuen Empfänger ein und ändern Sie ggf. den Betreff ab bevor Sie die E-Mail senden.

##### Outlook 365 und 2010/2013/2016

1. Öffnen Sie die E-Mail, die weitergeleitet werden soll.
2. Wählen Sie in der Multifunktionsleiste „**Antworten** > **Weitere** > **Als Anlage weiterleiten**“. Eine neue E-Mail wird erzeugt.
3. Tragen Sie den neuen Empfänger ein und ändern Sie ggf. den Betreff ab bevor Sie die E-Mail senden.

##### Apple Mail unter macOS

1. Öffnen Sie die E-Mail, die Sie als Anhang weiterleiten möchten.
2. Wählen Sie in der Menüleiste „**E-Mail** > **Als Anhang weiterleiten**“. Eine neue E-Mail wird erzeugt.
3. Tragen Sie den neuen Empfänger ein und ändern Sie ggf. den Betreff ab bevor Sie die E-Mail senden.

### Was geschieht mit den Meldungen

Wir lesen diese Daten in unseren lokalen Spamfilter ein, sodass in Zukunft mit weniger Spam-Nachrichten zu rechnen ist. Bitte beachten Sie, dass diese Lösung einige Zeit braucht, um bemerkbar zu werden. Eine schnellere Lösung ist der Wechsel der E-Mail-Adresse unter [mein.liwest.at](https://mein.liwest.at).

#### Ratschläge:

Anzuraten ist auch ein bedachter Umgang mit Ihrer Adresse: Sofern Sie sich bei Newslettern anmelden, werden Ihre Daten an Dritte weitergegeben, welche wiederum Werbemails versenden. Sofern dies schon passierte, achten Sie auf den Fuß der E-Mail: Eventuell steht hier ein ähnlicher Text wie „Abmelden“ oder „Unsubscribe“, welchen Sie anklicken können, um sich aus den Verteilern entfernen zu lassen.

Ebenfalls mehren sich Meldungen zu Einbrüchen bekannter Webseiten, bei welchen persönliche Daten abgegriffen und verkauft werden. Um nachzuvollziehen, ob ein bekannter „Leak“ stattgefunden hat, prüfen Sie Ihre E-Mail-Adresse auf der Seite [haveibeenpwned.com](https://haveibeenpwned.com)

Werden nun Einträge angezeigt, ist ein Wechsel der Adresse der beste Weg.

- Geben Sie ihre E-Mail-Adresse nur an Personen weiter, denen Sie vertrauen.
- Nutzen Sie Ihre E-Mail-Adresse nicht bei Gewinnspielen, da diese Daten (siehe Kleingedrucktes) zu Werbezwecken vermarktet werden können.
- Verwenden Sie auf Webseiten ein sicheres Passwort, damit ein Auslesen der Daten durch einen Angriff erschwert wird. Oftmals sind persönliche Daten mehr wert, als Ihnen bewusst ist.

Wie Sie ein sicheres Passwort erstellen, erfahren Sie unter [www.datenschutz.org/sicheres-passwort/](https://www.datenschutz.org/sicheres-passwort/)