











Verwenden Sie diese Checkliste am Arbeitsplatz bzw. auch privat. Sie hilft Ihnen, Angriffen auf Ihre Daten (und jene Ihrer Arbeitskolleginnen und -kollegen) aktiv vorzubeugen. Sie erfüllen damit den wichtigsten Beitrag zur IT-Sicherheit: **Schutz Ihrer digitalen Identität.**

Tipp:

Aussendungen von IT-SERVICES überprüfen Sie im Intranet: [swa.wu.ac.at/it-services-aussendungen](https://short.wu.ac.at/it-services-aussendungen)

Bitte prüfen Sie den Gesamteindruck*	JA	NEIN
Ist Ihnen die E-Mail-Adresse der Absenderin bzw. des Absenders vertraut ?	<input checked="" type="checkbox"/>	
Ist der Betreff bzw. das geäußerte Anliegen von dieser Adresse zu erwarten ?	<input checked="" type="checkbox"/>	
Wird eine generische Anrede anstelle einer persönlichen Anrede verwendet? <i>z.B. Liebe Kundin, Lieber Kunde, Sehr geehrter Kontoinhaber, Hallo, ...</i>		<input checked="" type="checkbox"/>
Passt die verwendete Sprache zum Absender bzw. Empfänger? <i>z.B. englischer Text oder Betreff an/von deutschsprachigen Empfänger/Absender</i>	<input checked="" type="checkbox"/>	
Enthält die Nachricht zahlreiche Rechtschreib- oder Grammatikfehler ?		<input checked="" type="checkbox"/>
Wird die Dringlichkeit eines Anliegens hervorgehoben? Wird mit unangenehmen Konsequenzen gedroht?		<input checked="" type="checkbox"/>
Sind die geschilderten Sachverhalte oder Konsequenzen unüblich bzw. übertrieben ?		<input checked="" type="checkbox"/>
Werden firmeninterne Details bzw. Zugangsdaten angefordert?		<input checked="" type="checkbox"/>
Werden Sie zum Öffnen eines Links oder URLs aufgefordert?		<input checked="" type="checkbox"/>
Ist zusätzlich (mindestens) ein Dateianhang vorhanden? Achtung: auch übliche Dateiformate können bösartigen Code transportieren		<input checked="" type="checkbox"/>

* bei Telefongesprächen auf Rufnummer, anrufende Person und Gesprächsinhalt anwendbar

Legende**Alltägliche Kommunikation**

Achten Sie bitte dennoch auf die Sicherheitsempfehlungen: <https://short.wu.ac.at/sichere-it>
Danke!

**Sicherheitsrisiko!**

Überprüfen Sie auf anderen Wegen, ob die Nachricht von der genannten Person stammt.
(z.B. Webseite, Helpdesk bzw. Servicecenter, telefonische oder persönliche Nachfrage)

**Hohes Sicherheitsrisiko!**

- Löschen Sie die E-Mail Nachricht aus Posteingang **und** Papierkorb.
- Beenden Sie das Telefongespräch mit Hinweis auf die Informationssicherheit.

Uuups! Daten in falschen Händen?

- Bitte melden Sie Vorfälle und Mängel betreffend IT- und Informationssicherheit umgehend an: hotline@wu.ac.at.
- Behalten Sie nach Ihrer Meldung alle E-Mails und andere Daten. Löschen Sie nichts! Schalten Sie die betroffenen Geräte sofort ab und lassen Sie diese deaktiviert.