Sichere E-Mail
- wie man Phishing vermeidet -

RUHR UNIVERSITÄT BOCHUM

Stabsstelle für Informationssicherheit

Der 3-Sekunden-Sicherheitscheck:

- Ist die Absender-Adresse **bekannt**?
- Wird ein Dokument von diesem Absender **erwartet?**
- Sind Betreff und Inhalt der E-Mail **sinnvoll**?
- Weist der Link auf ein Ziel, das Sie erwarten würden?

➔ Wenn Sie diese Fragen überwiegend verneinen, handelt es sich wahrscheinlich um Spam oder eine Phishing-E-Mail!

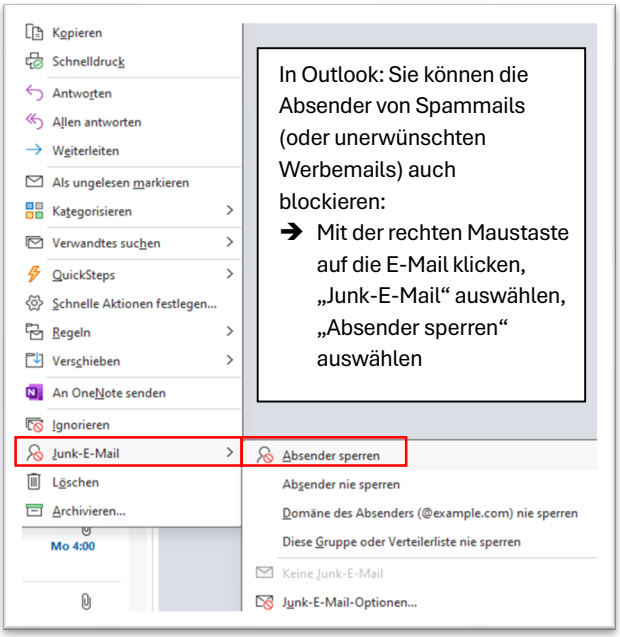
Spam-E-Mails und andere unerwünschte E-Mails sollten Sie ignorieren und löschen.

Nutzende von RUB-Mail sollten Spam- und Phishing-Mails in den Ordner UCE-TMP verschieben. So wird der Spam-Filter der RUB trainiert und die Mail später automatisch gelöscht.

E-Mail-Anhänge oder Links können ein Schadprogramm enthalten, das sich beim Öffnen der angehängten Datei selbstständig lädt und den Rechner infiziert.

Schadprogramme „verstecken“ sich oft hinter Formaten wie z.B. .exe, .bat, .zip, .js., .scr, .docm, .xlsm oder alten Formaten wie .doc oder .xls. Als E-Mail-Anhänge werden diese Formate blockiert. Bei Download-Links muss man selbst Acht geben. Auch HTML-Dateien im Anhang sind häufig schädlich.

Seien Sie wachsam. Fragen Sie lieber nach und fordern Sie Dokumente im PDF-Format oder als JPG/PNG an. Teilen Sie Dokumente im Fileshare (innerhalb der RUB) oder z.B. über sichere Dienste wie Sciebo (außerhalb der RUB).



1.1. Dos

- Spamfilter einschalten (RUB-Mail)
- Links überprüfen (mit der Maus über den Link fahren)
- Eingabe von Zugangsdaten NUR auf zweifelsfrei echten RUB-Seiten oder zweifelsfrei identifizierten externen Seiten
- Verkürzte Links und QR-Codes vor dem Klicken überprüfen

Don´ts

- Nicht unter Druck setzen lassen
- Keine Weiterleitung an private E-Mailadressen
- Kein unverschlüsselter Versand vertraulicher Informationen an E-Mailempfänger außerhalb der RUB
- Kein Unsubscribe/Abbestellen vonSpam-/Werbemails
- Spammern niemals antworten