



## **Aus- und Fortbildungszentrum** **Kompetenzzentrum E-Government**

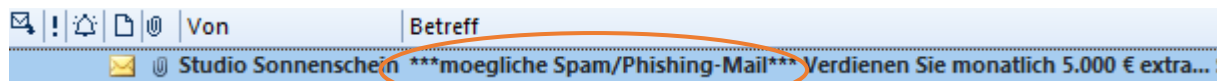
### **Outlook: Umgang mit Spam / Phishing-Mail**

#### **Spam**

In den letzten Jahren hat die Zahl unerwünschter Massen-E-Mails und Postings sog. "Spam" (engl. to spam umgangssprachlich "zumüllen") stark zugenommen. Meist handelt es sich dabei um Werbung, die sich im elektronischen Briefkasten sammelt. Die Skala reicht dabei von lästig bis bedrohlich.

Verdächtige Spam-Mails werden von Dataport automatisch mittels eines Prüfverfahrens identifiziert und im Betreff als mögliche Spam/Phishing-Mail gekennzeichnet. Sie dürfen aber aus rechtlichen Gründen nicht gelöscht werden, da im automatisierten Verfahren lediglich eine erhöhte Wahrscheinlichkeit ermittelt werden kann.

Die Kennzeichnung erfolgt im Betreff vorangestellt: **\*\*\*moegliche Spam/Phishing Mail\*\*\***



Der E-Mailempfänger muss letztendlich prüfen und entscheiden, was mit dieser verdächtigen E-Mail passieren soll.

#### **Phishing**

Unter Phishing (Kunstbegriff aus Password und fishing) versteht man das Ausspionieren von Anwendern. Dabei werden Kennwörter und persönliche Daten ausgelesen und zu kriminellen Zwecken missbraucht. In E-Mails und auf Webseiten werden dazu kleine Programme platziert, die vom Benutzer unbemerkt ihre verdeckte Spionageaufgabe ausführen.

Im Bremer Verwaltungsnetz werden zum Schutz der Anwender Filtersysteme eingesetzt, die gefährliche E-Mails bereinigen. Meistens lauert die Gefahr in den Anlagen. Diese werden, soweit sie erkannt werden, aus der E-Mail entfernt.

Da ständig neue Varianten dieser Bedrohung auftreten, ist es wichtig, dass alle die entsprechende Vorsicht walten lassen. E-Mails, die Ihnen verdächtig vorkommen, sollten Sie nicht öffnen und diese stattdessen melden!

#### **Falsche Absender**

Die Angaben zum Absender einer E-Mail können gefälscht bzw. vertauscht worden sein. Seien Sie deshalb vorsichtig und kontrollieren Sie die E-Mail kurz, bevor Sie diese öffnen.

#### **Herausgeber**

Aus- und Fortbildungszentrum für den bremischen öffentlichen Dienst  
Doventorscontrescarpe 172C  
28195 Bremen



Merkwürdige Betreffs oder ungewöhnliche Zeitstempel sind bereits Indiz für diese Form eines Angriffs. Im Zweifel kontaktieren Sie den Absender und versichern sich der Korrektheit der E-Mail.

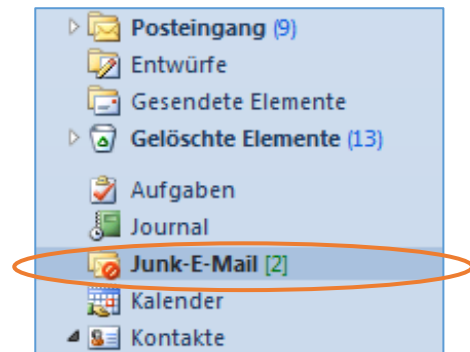
Die falschen Absender können leider im automatisierten Verfahren nicht erkannt werden.

## Der Ordner Junk-E-Mail für Spam/Phishing-Mail

Vorsichtshalber soll eine verdächtige Mail in den Ordner **Junk-E-Mail** verschoben und wenn überhaupt nur dort geöffnet werden.

Dieser Ordner bietet einen besonderen Schutz gegen unvorsichtiges Öffnen von E-Mails im HTML- oder RTF-Format sowie von Hyperlinks und Anlagen.

Die E-Mail wird nur im Textformat geöffnet. Dabei werden die möglichen Formatierungen der ursprünglichen E-Mail ausgeblendet. Hyperlinks und Anlagen können in dem Ordner **Junk-E-Mail** gar nicht geöffnet werden.



Wenn Sie eine E-Mail im Ordner Junk-E-Mail öffnen, bekommen Sie am oberen Rand der E-Mail je nach Inhalt eine entsprechende Meldung:

Hyperlinks und sonstige Funktionen wurden in dieser Nachricht deaktiviert. Verschieben Sie die Nachricht in den Posteingang, um die Funktionen wiederherzustellen.

Diese Nachricht wurde zum Nur-Text-Format konvertiert.

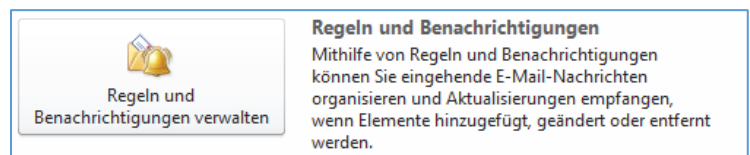
Outlook hat den Zugriff auf die folgenden potenziell unsicheren Anlagen blockiert: Handreichung ... .pdf, Sprachliche Feinheiten ... .docx.

Wenn die E-Mail sich als unproblematisch erweist und Sie diese vollständig lesen und bearbeiten möchten, schieben Sie die E-Mail in den Ordner **Posteingang**.

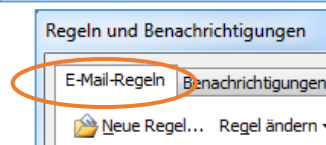
## E-Mail Regel im Regel-Assistenten erstellen

Dataport kennzeichnet verdächtige E-Mails mit dem Zusatz **\*\*\*mögliche Spam/Phishing-Mail\*\*\***. Diese können Sie in Outlook mit Hilfe einer Regel automatisch beim Eintreffen von Ihrem Posteingang in den Ordner **Junk-E-Mail** verschieben lassen.

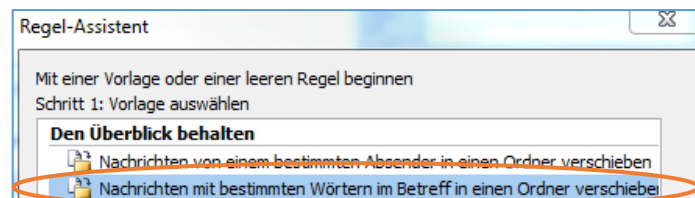
Wählen Sie im Menüband unter **Datei > Informationen > Regeln und Benachrichtigungen verwalten**.



Klicken Sie auf **Neue Regel...**

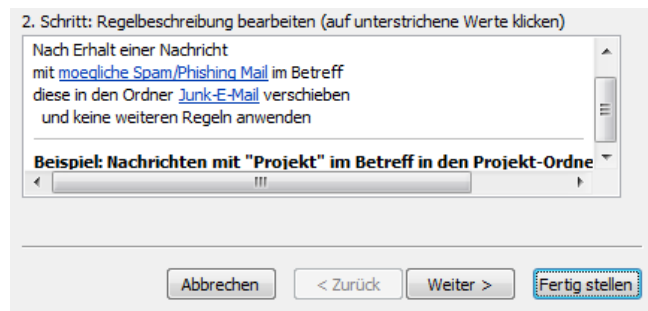


Im Regel-Assistenten finden Sie unter **Schritt 1: Vorlagen auswählen** die Vorlage **Nachrichten mit bestimmten Wörtern im Betreff in einen Ordner verschieben**.



Im 2. Schritt: **Regelbeschreibung bearbeiten** klicken Sie auf [bestimmten Wörtern](#) –und tragen sie den gesuchten Text moegliche Spam/Phishing Mail ein. Danach klicken Sie auf [Zielordner](#) und wählen den **Ordernamen Junk-E-Mail** aus.

Dann wählen Sie **Fertig stellen**.



### Hinweis zur "sssss-Regel"

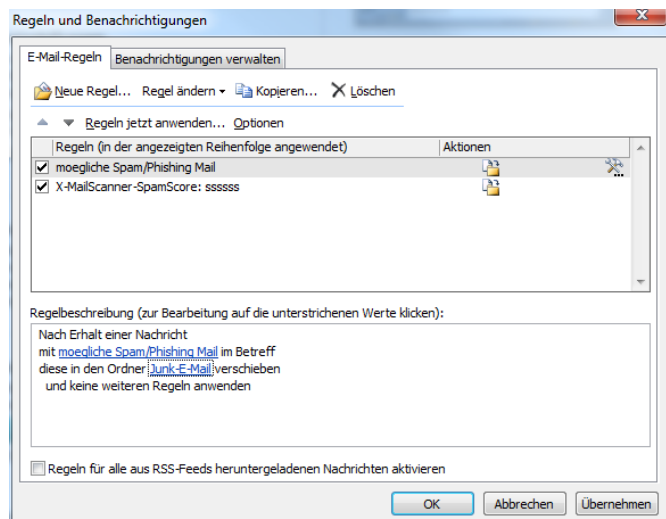
Sie können auch eine Regel definieren, die im Betreff nach **sssss** sucht und diese in den **Junk-E-Mail** Ordner verschieben lassen. Die "sssss" werden bei dem automatisierten Prüfverfahren zusätzlich in der Kopfzeile (siehe Datei > Information > Eigenschaften > Internetkopfzeilen) der verdächtigen E-Mail als Kennzeichen für Spam/Phishing hinterlegt.

Wenn Sie eine entsprechende Regel wie oben beschrieben erstellt haben, erscheint diese in der Liste. Klicken Sie abschließend auf **OK**.

Wenn Sie auf **Regel jetzt anwenden...** klicken, können Sie die Regeln nachträglich für bereits empfangene Mails anwenden.

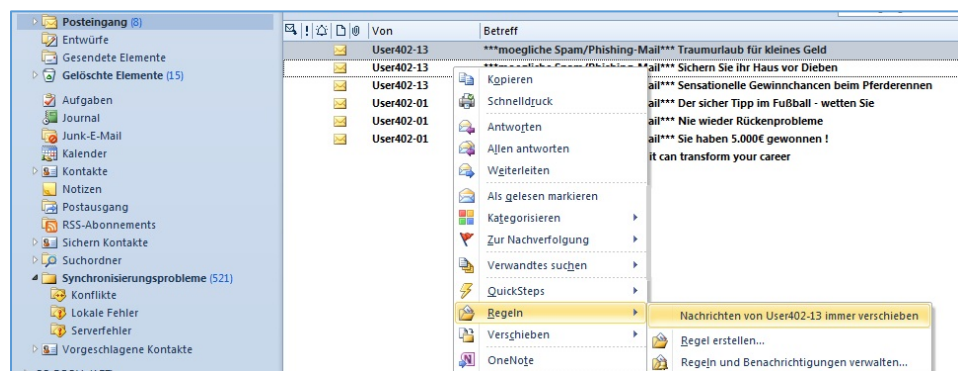
Regeln können nachträglich geändert oder gelöscht werden.

Mehrere Regeln müssen in einer sinnvollen Reihenfolge definiert werden, um Konflikte auszuschließen.



### Regeln direkt im Posteingang erstellen

Wenn Sie eine unerwünschte E-Mail im Posteingang, im Ordner Junk-E-Mail oder einem anderen Ordner Ihres Postfaches finden, können Sie für diese E-Mail direkt eine Regel erstellen.

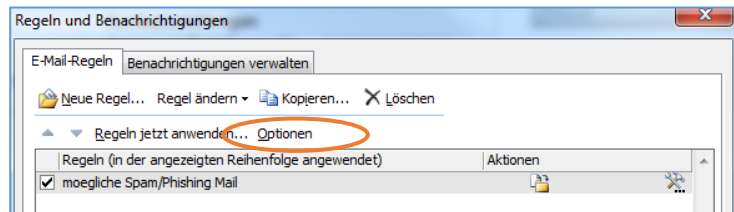


Häufig bezieht sich eine derartige Regel auf den Absender. Es werden dann alle E-Mails dieses Absenders in einen Zielordner **Junk-E-Mail** verschoben.

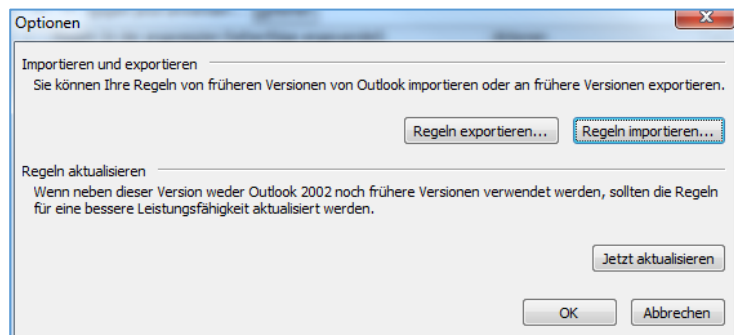
### Regeln importieren und exportieren

Ihre Dienststelle oder andere Personen können Ihnen eine Datei (Endung \*.rwz) mit Regeln zur Abwehr unerwünschter E-Mail zur Verfügung stellen. Diese können Sie in Outlook importieren.

Unter **Datei > Regeln und Benachrichtigungen verwalten** klicken Sie auf **Optionen**.

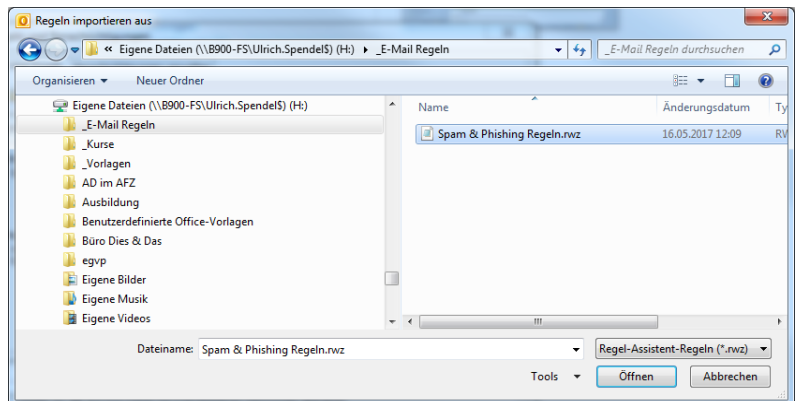


Wählen Sie **Regeln importieren**.



Navigieren Sie in das entsprechende Verzeichnis und markieren Sie die Datei mit der Endung \*.rwz.

Klicken sie auf **Öffnen**.



Die importierten Regeln werden in die Liste der Regeln aufgenommen.

Dabei wird nicht geprüft, ob es eine Regel schon gibt. Kontrollieren Sie deshalb das Ergebnis.

Damit die Regeln auch tatsächlich wirken, kontrollieren Sie auch die Reihenfolge.

### Exportieren vorhandener Regeln

Regeln, die Sie in Ihrem Outlook erstellt oder importiert haben, können Sie auch anderen zur Verfügung stellen. Dazu wählen Sie **Regeln exportieren**. Dabei können Sie wählen, ob alle oder nur ausgewählte Regeln exportiert werden sollen. Geben Sie einen Dateinamen an, die Endung \*.rwz wird automatisch angefügt.