# *E-Mail*



## 1. Überblick

In diesem Dokument werden sicherheitsrelevante Einstellungen für verschiedene *E-Mail*-Programme vorgestellt. Die *E-Mail*-Programme, die auf Rechnern der Hochschule Fulda eingesetzt werden, müssen entsprechend konfiguriert werden. Falls auf einem Rechner der Hochschule Fulda ein *E-Mail*-Programm eingesetzt wird, das in diesem Dokument nicht enthalten ist, müssen die entsprechenden Einstellungen in dem Programm in analoger Weise vorgenommen werden und der Name des Programms muss dem bzw. der IT-Sicherheitsbeauftragten der Hochschule mitgeteilt werden.

Eine *E-Mail* sollte immer nur als normaler Text versendet werden, da im *HTML-Code* Schadensfunktionen enthalten sein können, die den Rechner kompromittieren. Klicken Sie nie auf *HTML*- oder *Office*-Dokumente in Anhängen, wenn die *E-Mail* nicht von einer vertrauenswürdigen Quelle stammt. Falls Sie einen formatierten Text versenden wollen, sollten Sie ihn als Anlage senden und in Ihrer *E-Mail* explizit auf diese Anlage hinweisen.

**Denken Sie daran, dass Absenderadressen von *E-Mails* gefälscht sein können und dass *Malware-E-Mails* immer ausgeklügelter werden.** *Malware-E-Mails* werden heute bereits sehr oft in gutem Deutsch oder Englisch verschickt und haben eine Absenderadresse, die dem Empfänger bekannt ist. Inzwischen gibt es noch raffiniertere Fälschungen, die auf *E-Mails* antworten, die man dem vorgetäuschten Absender tatsächlich einmal geschickt hat. Dies wird dadurch möglich, dass *E-Mails* von infizierten Rechnern gelesen und zumindest teilweise an Kriminelle übertragen werden, sodass sie die Informationen zu Absender, Empfänger, Betreff und ggf. sogar die Nachricht selbst kennen und für ihre *Malware-E-Mail* benutzen können. Auf diese Weise können dann die Bekannten des ersten Opfers angegriffen werden, da die *Malware-E-Mail* als Antwort auf eine eigene *E-Mail* sehr glaubwürdig ist.

**Klicken Sie möglichst nie auf *Links* in *E-Mails*,** da sich hinter dem angezeigten und vertrauenswürdigen Text unter Umständen eine ganz andere Adresse verbirgt (statt "https://.../download/bericht.pdf" zum Beispiel "https://.../download/malware.exe"). Es wird inzwischen auch versucht, Schad-Software zum Beispiel als verschlüsseltes ZIP-Archiv zu verschicken, für das das Passwort zum Entschlüsseln in der *E-Mail* mitgeteilt wird. Auf diese Weise kann ein *Anti-Virenprogramm* die Schad-Software im Anhang der *E-Mail* nicht erkennen, während der Empfänger das Archiv öffnen und die Schad-Software ausführen kann (eventuell kann das *Anti-Virenprogramm* die Ausführung der Schad-Software jetzt noch verhindern).

**Prüfen** Sie *Links* in *E-Mails* sehr genau, bevor Sie darauf klicken (in der Regel wird die Adresse in der unteren Statuszeile des *E-Mail-Clients* angezeigt, wenn Sie mit dem Mauszeiger auf den *Link* gehen), wenn das Klicken auf den *Link* unbedingt sein muss. **Prüfen** Sie den Dateityp eines Anhangs und klicken Sie nie auf ausführbare Dateien (.exe, .bat, .com, .msi, ...). **Verbieten** Sie Makros in *Office*-Dokumenten (Office_Makros_deaktivieren.pdf) und erlauben Sie sie auf keinen Fall, wenn ein als Anhang empfangenes *Office*-Dokument es fordert. **Fragen** Sie telefo-

nisch beim Absender der *E-Mail* nach, ob er Ihnen die Nachricht mit den Anhängen geschickt hat, wenn Sie sich unsicher sind, bevor Sie einen Anhang benutzen oder auf einen *Link* klicken.

**Seien Sie besonders vorsichtig**, wenn Sie in einer *E-Mail* im Anhang Dateien mit den folgenden Dateinamenerweiterungen erhalten, da solche Dateien Schad-Software enthalten können.

| **Datei** | **Dateinamenerweiterung** |
|---|---|
| Makrofähige Microsoft Word Dokumente oder Vorlagen bis *Word 2003* | .doc, .dot |
| Makrofähige Microsoft Word Dokumente oder Vorlagen ab *Word 2007* | .docm, .dotm |
| Makrofähige Microsoft Excel Arbeitsmappen, Erweiterungsmodule (Add-In) oder Vorlagen bis *Excel 2003* | .xls, .xla, .xlt |
| Makrofähige Microsoft Excel Arbeitsmappen, Binärarbeitsmappen, Erweiterungsmodule (Add-In) oder Vorlagen ab *Excel 2007* | .xlsm, .xlsb, .xlam, .xltm |
| Makrofähige Microsoft PowerPoint Präsentationen, Erweiterungsmodule (Add-In) oder Vorlagen bis *PowerPoint 2003* | .ppt, .ppa, .pot |
| Makrofähige Microsoft PowerPoint Präsentationen, Bildschirmpräsentationen, Folien, Erweiterungsmodule (Add-In) oder Vorlagen ab *PowerPoint 2007* | .pptm, .ppsm, .sldm, .ppam, .potm |
| Ausführbare Programme | .com, .exe, .msc, .msi, .mst, .scr |
| Ausführbare Skriptdateien | .bat, .cmd, .js, .jse, .ps1, .vba, .vbe, .vbs, .ws, .wsf, .wsh |
| Verknüpfungen | .lnk |
| Control Panel Programme, Windows Jobs, ActiveX-Steuerelemente, Registry-Einträge, Systemgerätetreiber, Microsoft Compiled/Compressed HTML Hilfe-Dateien, Microsoft HTML-Anwendungen, Programminformationsdateien, Shell Command Files | .cpl, .job, .ocx, .reg, .sys, .chm, .hta, .pif, .scf |
| (verschlüsselte) Archive (insbesondere, wenn Ihnen das Passwort zum Öffnen des Archivs in der *E-Mail* mitgeteilt wird) | .zip, .jar, .cab, .gz, .7z, .tgz |

Sie sollten *Windows* so konfigurieren, dass Dateinamenerweiterungen auch im Dateimanager (*Windows-Explorer*) angezeigt werden (standardmäßig werden sie nicht angezeigt). Klicken Sie mit der rechten Maustaste auf das *Windows-Symbol* in der linken unteren Ecke des Bildschirms, wählen Sie den Eintrag *Suchen* aus, geben Sie im Suchfeld den Wert *Explorer-Optionen* ein und klicken Sie dann auf den Eintrag *Explorer-Optionen Systemsteuerung*. Wählen Sie im neuen Fenster den Reiter *Ansicht* und entfernen Sie den Haken vor dem Eintrag *Erweiterungen bei bekannten Dateitypen ausblenden*. Klicken Sie dann auf *Übernehmen* und danach auf *OK*.

Einige *E-Mail*-Programme erlauben, automatische Bestätigungen für den Empfang der *E-Mail* anzufordern. Diese Eigenschaft kann für *Spam-E-Mail* missbraucht werden, da der Absender der *E-Mail* dann weiß, dass die Adresse noch benutzt wird und für *Spam-E-Mail* ideal geeignet ist. Sie sollten diesen Mechanismus deshalb abschalten. Falls Sie Bestätigungen für den Empfang

einer Nachricht zulassen wollen, sollten Sie auf jeden Fall einstellen, dass Sie gefragt werden, bevor die Bestätigung versendet wird.

**Speichern Sie niemals Passwörter in Programmen oder Dateien**, weil Sie zu bequem sind, das Passwort jedes Mal wieder einzugeben. Da Schad-Software die im Klartext abgelegten Passwörter finden und sammeln kann, laden Sie alle potenziellen "Hacker" geradezu ein, Ihre Benutzerkennung zu missbrauchen. Die Sicherheit wird erhöht, wenn Sie alle Passwörter mit einem *Master-Passwort* verschlüsseln. Die verschlüsselten Passwörter können allerdings ebenfalls gesammelt und ggf. auf leistungsfähigen Rechnern durch Ausprobieren "geknackt" werden.

In *Cookies* werden Sitzungsprotokolle gespeichert, die für *E-Mail* nicht erforderlich sind. Aus diesem Grund sollte dieser Dienst für *Mail- & News*-Gruppen abgeschaltet werden. *Cookies* können auch missbraucht werden, um ein Profil des Benutzers bzw. der Benutzerin zu erstellen, das dann für gezielte *Spam-E-Mails* benutzt werden kann.

Da eine *E-Mail* nur normalen Text enthalten soll, sollten aus Sicherheitsgründen *JavaScript* und *Plugins* für *E-Mails* abgeschaltet werden. Falls Sie aktive Elemente benötigen, sollten Sie sie als Anlage in einer Datei senden und auf die Anlage explizit hinweisen.

**Öffnen Sie niemals den Anhang einer *E-Mail*, bevor Sie ihn auf *Viren, Würmer, Trojaner, ...* untersucht haben.**

In den Einstellungshinweisen ab Kapitel 3 bedeutet "Bearbeiten > ... > ...", dass Sie im entsprechenden Eintrag der Menüzeile am oberen Rand des Programmfensters beginnen (z. B. "Bearbeiten" oder "Extras") und dann mit einem Eintrag des Menüs, einem Karteikartenreiter oder einem anderen Element weitermachen, das die entsprechende Beschriftung aufweist.

Seitenanfang

## 2. *Spam-E-Mail*

Einen guten Überblick über diese Thematik finden Sie beispielsweise bei Wikipedia. In der Hochschule Fulda werden *Spam-E-Mails* von einem *Spam*-Filter durch das Schlüsselwort "<?SPAM?>" im *Subject:*- bzw. *Betreff:*-Feld gekennzeichnet. In sehr seltenen Fällen kann es vorkommen, dass eine normale *E-Mail* als *Spam* klassifiziert wird. Bei *Spam-E-Mail* sollten Sie Folgendes beachten:

1. Erlauben Sie keine (automatischen) Bestätigungen, damit sich Ihre *E-Mail*-Adresse nicht als aktive *E-Mail*-Adresse beim Absender "meldet" und Sie danach noch mehr *Spam-E-Mail* erhalten.
2. Löschen Sie die *E-Mail*, ohne sie zu lesen oder zu beantworten.
3. Klicken Sie auf keine Anhänge von *Spam-E-Mail*.
4. Klicken Sie auf keinen Fall auf irgendwelche Web-Adressen in der *Spam-E-Mail*, über die Sie angeblich in Zukunft solche *E-Mails* vermeiden können, da Sie dadurch nur eine aktive *E-Mail*-Adresse "anmelden" und demnächst noch mehr *Spam-E-Mail* erhalten.
5. Benutzen Sie Ihre *E-Mail*-Adresse niemals für Preisausschreiben oder Ähnliches, da Sie damit unter Umständen *Spam-E-Mails* veranlassen. Richten Sie sich für solche Dinge eine kostenfreie *E-Mail*-Adresse bei irgendeinem *Provider* ein, die Sie anschließend wieder löschen können.
6. Tarnen Sie Ihre *E-Mail*-Adresse auf Ihren Web-Seiten, damit sie von Suchprogrammen nicht gefunden wird und dann *Spam*-Adresslisten hinzugefügt werden kann.

Seitenanfang

# 3. Mozilla

## 3.1. Thunderbird 91.x

*Thunderbird* will große Anhänge auf einem *Cloud-Storage-Server* im Internet speichern und in der *E-Mail* nur noch die Adresse der Datei angeben. Damit können zwar problemlos sehr große Dateien per *E-Mail* verschickt werden, aber man hat keinen Einfluss darauf, was mit der Datei auf dem *Server* passiert (Dauer der Speicherung, Datenschutz, usw.).

Sie können mit der rechten Maustaste in die "Titelzeile" (der Hintergrund am oberen Rand neben dem "*Tab*") klicken und "Menüleiste" auswählen, um die "alte" Darstellung zu erhalten, in der Sie dann in der Menüleiste auf "Extras > Einstellungen" klicken. Alternativ können Sie in der rechten oberen Ecke auf das *Icon* mit den drei waagerechten Linien und dann auf "Einstellungen" klicken. Die folgenden Auswahlhinweise setzen ein geöffnetes Einstellungsfenster voraus. Es sollten folgende Einstellungen vorgenommen werden:

1. Auf der linken Seite "Allgemein" auswählen.
    - Auf der rechten Seite am Ende des Abschnitts "Lesen & Ansicht" bei "Den Umgang mit Empfangsbestätigungen (MDN) in Thunderbird festlegen" auf "Empfangsbestätigungen..." klicken und dann "Nie eine Empfangsbestätigung senden" auswählen.
    - Auf der rechten Seite im Abschnitt "Thunderbird-Updates" sollte bei "Thunderbird erlauben" der Eintrag "Updates automatisch zu installieren (empfohlen: erhöhte Sicherheit)" ausgewählt sein oder ausgewählt werden.
2. Auf der linken Seite "Verfassen" auswählen.
    - Auf der rechten Seite im Abschnitt "HTML-Optionen" bei "Verhalten beim Senden von HTML-Nachrichten:" auf "Sendeoptionen..." klicken und dann im Abschnitt "Textformat" die Aktion "Nachrichten falls möglich als Reintext senden" auswählen. Für "Beim Senden von Nachrichten im HTML-Format an Empfänger, die laut Liste HTML nicht empfangen können oder wollen:" den Eintrag "Nachrichten in reinen Text konvertieren" auswählen.
    - Auf der rechten Seite sollte im Abschnitt "Anhänge" der Haken vor "Hochladen für Dateien größer als xx MB anbieten" entfernt werden.
3. Auf der linken Seite "Datenschutz & Sicherheit" auswählen.
    - Auf der rechten Seite im Abschnitt "E-Mail-Inhalte" sollte der Haken vor "Externe Inhalte in Nachrichten erlauben" fehlen oder entfernt werden.
    - Auf der rechten Seite sollten im Abschnitt "Webinhalte" folgende Einstellungen vorgenommen werden.
        - Die Haken vor "Besuchte Webseiten und Links merken" und vor "Cookies von Webseiten akzeptieren" sollten fehlen oder entfernt werden.
        - Vor "Websites eine "Do Not Track"-Mitteilung senden, dass Ihre Online-Aktivitäten nicht verfolgt werden sollen" sollte ein Haken gesetzt sein oder gesetzt werden.
    - Auf der rechten Seite können im Abschnitt "Passwörter" alle gespeicherten "Passwörter" über "Gespeicherte Passwörter..." gelöscht werden. Es sollten nie Passwörter gespeichert werden.
    - Auf der rechten Seite sollten im Abschnitt "Datenerhebung durch Thunderbird und deren Verwendung" folgende Einstellungen vorgenommen werden.

        - Der Haken vor "Thunderbird erlauben, Daten zu technischen Details und Interaktionen an Mozilla zu senden" sollte fehlen oder entfernt werden.
        - Der Haken vor "Nicht gesendete Absturzberichte automatisch von Thunderbird senden lassen" sollte fehlen oder entfernt werden.
    - Auf der rechten Seite sollten im Abschnitt "Sicherheit" folgende Einstellungen vorgenommen werden.
        - Vor "Nachrichten auf Betrugsversuche (Phishing) untersuchen." sollte ein Haken gesetzt sein oder gesetzt werden.
        - Vor "Antivirus-Software ermöglichen, eingehende Nachrichten unter Quarantäne zu stellen." sollte ein Haken gesetzt sein oder gesetzt werden.
        - Vor "Aktuelle Gültigkeit von Zertifikaten durch Abfrage bei OCSP-Server bestätigen lassen" **muss** ein Haken gesetzt sein oder gesetzt werden.
4. Klicken Sie wieder in der rechten oberen Ecke auf das *Icon* mit den drei waagerechten Linien und dann auf "Konten-Einstellungen" oder direkt auf "Kontoeinstellungen" rechts oben im Hauptfenster. Alternativ können Sie auch "Extras > Konten-Einstellungen" auswählen, wenn Sie die Menüleiste aktiviert haben.
    - Auf der linken Seite "Server-Einstellungen" auswählen.
        - Im Abschnitt "Sicherheit und Authentifizierung" sollte unter "Verbindungssicherheit:" der Punkt "SSL/TLS" ausgewählt sein oder ausgewählt werden.
        - Unter "Authentifizierungsmethode:" sollte der Punkt "Passwort, normal" ausgewählt sein oder ausgewählt werden.
    - Auf der linken Seite "Verfassen & Adressieren" auswählen.

      Dort Haken vor "Nachrichten im HTML-Format verfassen" entfernen.
    - Auf der linken Seite "Postausgangs-Server (SMTP)" auswählen. Dann im rechten Fenster einmal auf den *Mail-Server* klicken und danach "Bearbeiten..." wählen.
        - Unter "Verbindungssicherheit:" sollte der Punkt "STARTTLS" ausgewählt sein oder ausgewählt werden.
        - Unter "Authentifizierungsmethode:" sollte der Punkt "Passwort, normal" ausgewählt sein oder ausgewählt werden.

Seitenanfang

# 4. Microsoft

## 4.1. Outlook 2010 bis 2013

Nachdem mit "Datei > Optionen" das Einstellungsfenster geöffnet worden ist, sollten folgende Einstellungen vorgenommen werden:

1. "E-Mail" auswählen.
    - Im Abschnitt "Nachrichten verfassen" in der Zeile "Nachricht in diesem Format verfassen:" den Eintrag "Nur-Text" auswählen.
    - Im Abschnitt "Verlauf" (weiter unten) sollte im Unterabschnitt "Für jede Nachricht, die die Anforderung einer Lesebestätigung enthält" die Zeile "Nie eine Lesebestätigung senden" ausgewählt sein oder ausgewählt werden.
2. "Personen" ("Kontakte" in *Outlook 2010*) auswählen.

   Im Abschnitt "Onlinestatus und Fotos" sollte der Haken vor "Benutzerfotos anzeigen, wenn verfügbar (...)" und vor "Nur Namen im Kontaktepopup (...) anzeigen" (fehlt in *Outlook 2010*) fehlen oder entfernt werden.
3. "Erweitert" auswählen.

   Im Abschnitt "Weitere" sollte der Haken vor "Die Analyse gesendeter E-Mails zulassen, um Personen, mit denen Sie häufig korrespondieren, ..., zu identifizieren und diese Informationen auf den Share-Point-Standardserver hochladen" fehlen oder entfernt werden.
4. "Sicherheitscenter > Einstellungen für das Sicherheitscenter..." bzw.
   "Trust Center > Einstellungen für das Trust Center..." auswählen.
    - Auf der linken Seite "E-Mail-Sicherheit" auswählen.
        - Im Abschnitt "Als Nur-Text lesen" sollte vor "Standardnachrichten im Nur-Text-Format lesen" ein Haken gesetzt sein oder gesetzt werden.
        - Im Abschnitt "Skript in Ordnern" darf vor "Skript in freigegebenen Ordnern zulassen" und vor "Skript in Öffentlichen Ordnern zulassen" kein Haken stehen.
    - Auf der linken Seite "Automatischer Download" auswählen.
        - Vor "Bilder in HTML-Nachrichten oder RSS-Elementen nicht automatisch herunterladen" sollte ein Haken gesetzt sein oder gesetzt werden.
        - Vor den vier Punkten "Download ..." sollten Haken fehlen oder entfernt werden, da Absenderadressen gefälscht sein können.
        - Vor "Warnhinweis anzeigen, bevor ..." sollte ein Haken gesetzt sein oder gesetzt werden.
5. In "Start" auf den kleinen *Pfeil nach unten* rechts vom *Icon* für "Junk-E-Mail" (letztes *Icon* in Spalte "Löschen") klicken. In dem sich öffnenden Fenster "Junk-E-Mail-Optionen..." auswählen. Im neuen Fenster den Reiter "Optionen" auswählen.
    - Dort ggf. auswählen, was mit *Spam/Junk-E-Mail* gemacht werden soll.
    - Vor "Hyperlinks und sonstige Funktionen in Phishingnachrichten deaktivieren (empfohlen)" sollte ein Haken gesetzt sein oder gesetzt werden (wird in *Outlook 2013* nur schwach dargestellt, sodass kein Haken gesetzt werden konnte).
    - Vor "Bei verdächtigen Domänennamen in E-Mail-Adressen warnen (empfohlen)" sollte ein Haken gesetzt sein oder gesetzt werden (wird in *Outlook 2013* nur schwach dargestellt, sodass kein Haken gesetzt werden konnte).

Seitenanfang

## 4.2. Outlook 2016, 2019 und 365

Office-2016-Produkte werden im Allgemeinen automatisch über *Windows-Update* aktualisiert. Bei Office 2019 und 365 muss das *Update* über ein Office-Programm angestoßen werden. Starten Sie zum Beispiel *Outlook 2019* oder *Outlook 365* und wählen Sie dann "Datei > Office-Konto" aus. Sie sollten auf der rechten Seite "Updates werden automatisch heruntergeladen und installiert" sehen. Wenn Sie auf "Updateoptionen" klicken, können Sie eine Überprüfung und ggf. Aktualisierung erzwingen, indem Sie auf " Jetzt aktualisieren" klicken.

Nachdem mit "Datei > Optionen" das Einstellungsfenster geöffnet worden ist, sollten folgende Einstellungen vorgenommen werden:

1. "Allgemein" auswählen (nur bei Office 2019 und Office 365 erforderlich).
    - Im Abschnitt "LinkedIn Funktionen" (am Ende auf der rechten Seite) sollte der Haken vor "LinkedIn-Funktionen in meinen Office-Anwendungen aktivieren" fehlen oder entfernt werden.
2. "E-Mail" auswählen.
    - Im Abschnitt "Nachrichten verfassen" in der Zeile "Nachricht in diesem Format verfassen:" den Eintrag "Nur-Text" auswählen.
    - Im Abschnitt "Verlauf" (weiter unten) sollte im Unterabschnitt "Für jede Nachricht, die die Anforderung einer Lesebestätigung enthält" die Zeile "Nie eine Lesebestätigung senden" ausgewählt sein oder ausgewählt werden.
    - Im Abschnitt "Nachrichtenformat" sollte für "Beim Senden von Nachrichten im Rich-Text-Format an Internetempfänger" der Wert "In Nur-Text-Format konvertieren" ausgewählt sein oder ausgewählt werden.
3. "Personen" auswählen.

    Im Abschnitt "Onlinestatus und Fotos" sollte der Haken vor "Benutzerfotos anzeigen, wenn verfügbar (...)" und vor "Nur Namen im Kontaktepopup (...) anzeigen" fehlen oder entfernt werden.
4. "Erweitert" auswählen.

    Im Abschnitt "Weitere" bzw. "Sonstige" sollte der Haken vor "Die Analyse gesendeter E-Mails zulassen, um Personen, mit denen Sie häufig korrespondieren, ..., zu identifizieren und diese Informationen auf den Share-Point-Standardserver hochladen" fehlen oder entfernt werden.
5. "Trust Center" und dann rechts "Einstellungen für das Trust Center..." auswählen.
    - Auf der linken Seite "Datenschutzoptionen" auswählen.
        - **Outlook 2016:**
            1. Vor "Persönliche Informationen an Microsoft senden, um bei der Verbesserung von Office zu helfen" sollte der Haken fehlen oder entfernt werden.
            2. Vor "Office-Verbindungen mit den Onlinediensten von Microsoft gestatten, ..." sollte der Haken fehlen oder entfernt werden.
        - **Outlook 2019 und 365:** Rechts "Datenschutzeinstellungen..." auswählen. Vor "Optionale verbundene Erfahrungen aktivieren" sollte der Haken fehlen oder entfernt werden.

- Auf der linken Seite "E-Mail-Sicherheit" auswählen.
  - Im Abschnitt "Als Nur-Text lesen" sollte vor "Standardnachrichten im Nur-Text-Format lesen" und vor "Digital signierte Nachrichten im Nur-Text-Format lesen" ein Haken gesetzt sein oder gesetzt werden.
  - Im Abschnitt "Skript in Ordnern" darf vor "Skript in freigegebenen Ordnern zulassen" und vor "Skript in Öffentlichen Ordnern zulassen" kein Haken stehen.
- Auf der linken Seite "Automatischer Download" auswählen.
  - Vor "Bilder in Standard-HTML-E-Mails oder RSS-Elementen nicht automatisch herunterladen" sollte ein Haken gesetzt sein oder gesetzt werden.
  - Vor den vier Punkten "Downloads ..." sollten Haken fehlen oder entfernt werden, da Absenderadressen gefälscht sein können.
  - Vor "Warnhinweis anzeigen, bevor ..." sollte ein Haken gesetzt sein oder gesetzt werden.
  - Vor "Bilder in verschlüsselten oder signierten HTML-E-Mails nicht herunterladen" sollte ein Haken gesetzt sein oder gesetzt werden.
- Auf der linken Seite "Makroeinstellungen" auswählen.
  - Es **muss** "Alle Makros ohne Benachrichtigung deaktivieren" ausgewählt sein oder ausgewählt werden.

6. Wählen Sie in der Titelzeile des Fensters "Start" aus.
   - **Outlook 2016:** Klicken Sie in der dritten Spalte auf den letzten Eintrag "Junk-E-Mail".
   - **Outlook 2019:** Klicken Sie in der dritten Spalte auf das *Icon* für "Junk-E-Mail".
   - **Outlook 365:** Klicken Sie am Ende der Titelzeile auf die drei Punkte ("Weitere Befehle") und dann auf den Eintrag "Junk-E-Mail".

   Wählen Sie den Eintrag "Junk-E-Mail-Optionen..." und dann im neuen Fenster den Reiter "Optionen" aus.
   - Dort ggf. auswählen, was mit *Spam/Junk-E-Mail* gemacht werden soll.
   - Vor "Hyperlinks und sonstige Funktionen in Phishingnachrichten deaktivieren (empfohlen)" sollte ein Haken gesetzt sein oder gesetzt werden (wird unter Umständen nur schwach dargestellt, sodass kein Haken gesetzt werden kann).
   - Vor "Bei verdächtigen Domänennamen in E-Mail-Adressen warnen (empfohlen)" sollte ein Haken gesetzt sein oder gesetzt werden (wird unter Umständen nur schwach dargestellt, sodass kein Haken gesetzt werden kann).

Seitenanfang

## 5. Novell GroupWise 2018 WebAccess Client

Wählen Sie "Werkzeuge" in der Menüleiste und dann den Eintrag "Optionen..." aus. Es sollten folgende Einstellungen vorgenommen werden:

1. Führen Sie einen Doppelklick auf "Umgebung" aus.
    - Wählen Sie den Reiter "Layouts" aus.

      Dort sollte als "Standardlayout & Schriftart beim Erstellen" und als "Standardlayout & Schriftart beim Lesen" ein Punkt vor "Einfacher Text" gesetzt sein oder gesetzt werden.
    - Wählen Sie den Reiter "Standardaktionen" aus.

      In den Abschnitten "Externe HTML-Bilder:" und "HTML-Skripte:" sollte ein Punkt vor "Warnung immer anzeigen" gesetzt sein oder gesetzt werden.
    - Wählen Sie den Reiter "Gestaltung" aus.

      Setzen Sie ggf. einen Haken vor "Blitzvorschau anzeigen", wenn Sie die Nachricht sofort lesen wollen.
2. Führen Sie einen Doppelklick auf "Senden" aus und wählen Sie dann den Reiter "Mail" aus.

   Im Abschnitt "Empfangsbestätigung" sollte in beiden Feldern der Wert "Keine" ausgewählt sein oder ausgewählt werden.

Seitenanfang

---

Letzte Änderung: 09. November 2021 | PDF-Version