

Quick Check für Bewerbungen

Vorgehensweise

- Bitte gehen Sie die Fragen der Reihe nach von oben nach unten durch.
- Sollte eine der Fragen mit JA beantwortet werden, dann handelt es sich möglicherweise um eine Phishing Mail und Sie sollten besonders achtsam sein.
- Bei Fragen oder wenn Sie sich unsicher sind, zögern Sie nicht das Informationssicherheitsteam oder den IT-Support (-2000) zu kontaktieren.



Die in der Email/Bewerbung angegebene Stelle ist NICHT ausgeschrieben?

- Handelt es sich ggf. um eine Initiativbewerbung?
- **Sollte auch dies nicht der Fall sein, empfehlen wir die Mail zu löschen.**

Soll die Bewerbung über einen Link geöffnet werden?

- Bei Links ist besondere Vorsicht geboten, da häufig nicht erkennbar ist, was dahintersteckt.
- Den Link sollten Sie auf keinen Fall öffnen.
- Sieht die Bewerbung ansonsten vertrauenswürdig aus, **bitte Sie den Bewerber Ihnen eine Datei zuzusenden.**



Ist die angehängte Datei verschlüsselt?



- Der Virens scanner kann Malware in passwortgeschützten Dateien nicht finden.
- Entschlüsseln Sie die Datei auf keinen Fall, da hierdurch die Malware direkt aktiv werden kann.
- Ausnahme sind verpackte & verschlüsselte Ordner wie .zip, .rar, u.ä.. Diese können entschlüsselt werden. Der Inhalt des Ordners ist im Anschluss jedoch zu prüfen.

Ist eine ausführbare Datei mit angehängt?

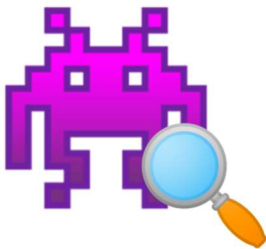
Hinter ausführbaren Dateien wie .bat, .cmd, .exe, usw. versteckt sich häufig Malware. **Diese auf keinen Fall öffnen!**

Aktivieren Sie die Dateiendungen im Explorer unter dem Reiter „Ansicht“ durch das Setzen des Hakens bei „Dateinamenerweiterung“.

Achten Sie auf versteckte Endungen wie „Foto.jpg.exe“ oder „Bewerbung.docx.cmd“.



Wurden beim Virenscan der Datei Malware gefunden?



- Über Rechtsklick auf die Datei kann man unter „Mit Windows Defender überprüfen...“ die Datei auf Malware prüfen.
- **Bei einem Fund verschieben Sie die Datei mit dem Windows Defender in Quarantäne und löschen die E-Mail.**

Möchte die Datei, dass Sie Makros oder den Bearbeitungsmodus aktivieren?

- Ihnen wird eine Meldung angezeigt, die besagt, dass die Datei angeblich mit einer älteren Version oder als Online Version erstellt wurden und Sie zum Betrachten den Bearbeitungsmodus und/oder Makros aktivieren sollen.
- **Folgen Sie dieser Meldung auf keinen Fall, sondern löschen die Datei und führen einen Virenscan Ihres Rechners durch**



Ihr Informationssicherheitsteam

- Bei Fragen und Anregungen Mail an: infosicherheit@uni-mannheim.de
- Sicherheitsvorfälle melden unter: itsupport@uni-mannheim.de
- Mehr Infos finden Sie auf: www.uni-mannheim.de/infosicherheit