

## ACHTUNG PHISHING: ES KÖNNTE AUCH SIE TREFFEN!

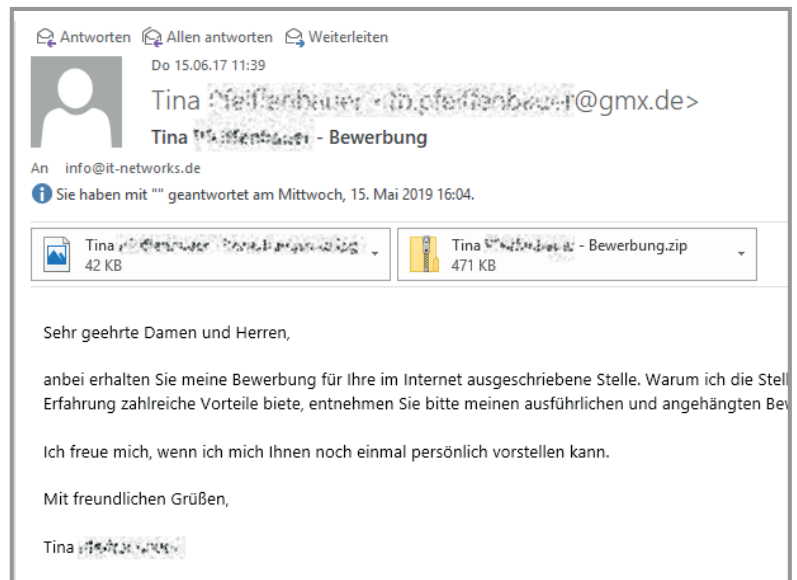
**Vorweg eine kurze Aufklärung:** unter dem Wort Phishing versteht man das (illegale) Vorhaben, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

### Aktuelle Maschen solcher Phishing-Mails:

- 📧 Restaurants erhalten Mails mit dem Fall einer angeblichen Lebensmittelvergiftung nach dem Restaurantbesuch, im Anhang Beweis-Foto und ärztliches Attest
- 📧 Bewerbungs-Mails mit Foto einer angeblichen Bewerberin und weiteren Dokumenten im Anhang
- 📧 Mails einer Rechtsanwaltskanzlei über angebliche offene Forderungen mit Benennung einer Bankverbindung zur Überweisung
- 📧 ein Hacker behauptet, auf den eigenen Mail-Account Zugriff zu haben und fordert eine Schutzgeldzahlung
- 📧 Amazon mit einer vermeintlichen Versandbestätigung
- 📧 Rechnungen von der Telekom und anderen Anbietern



**In Wirklichkeit  
enthalten die an-  
gehängten Office- oder  
PDF-Dokumente jedoch  
Viren und infizieren den  
Rechner des Empfängers  
mit Schadsoftware.**



### So können Sie eine Infizierung der Rechner erfolgreich vermeiden:

- ✓ Öffnen Sie keine Dateianhänge! Wenn der Urheber nicht bekannt ist, halten Sie besser vorher mit Ihrem EDV-Betreuer Rücksprache
- ✓ Erlauben Sie nicht das Ausführen von Makros beim Öffnen solcher Office-Dokumente (wie z. B. Word)!
- ✓ Sie können auch die Anhänge vorab auf dem Smartphone anschauen, da hier die Viren in der Regel nicht greifen
- ✓ Bleiben Sie immer schön wachsam und setzen Sie Ihren gesunden Menschenverstand ein!

Sollten Sie eine verdächtige Mail bekommen, können Sie gerne mit uns Kontakt aufnehmen, natürlich auch für Fragen zu anderen Themen im Zusammenhang mit Datenschutz und Datensicherheit.

### Ihre Datenschutzbeauftragte

**Madlen Rebel**

