# IT Info

**Mitarbeiter der IT**
**it@dfeug.de**

DFeuG
Deutsche Feuerwehr-Gewerkschaft

# SPAM MAILS

Spam-Mails und bösartige Verlinkungen innerhalb der Mailnachricht.

Seitdem es das Internet gibt, haben wir es mit verführerischen Angeboten zu tun oder mit Hackern, die auf fernen Rechnern, Spionage-Programme ausführen wollen. Die Methoden werden immer dreister und seit Beginn des Ukraine-Kriegs werden solche Attacken häufiger, weil sie Teil des Krieges sind.
Eine Verlinkung innerhalb solcher Mails kann zu Werbeinhalten oder einer Aktion führen, die der Spam-Absender verbreiten möchte.
Im schlechtesten Fall führen solche Links auf Webseiten, die dort einen Trojaner in Stellung bringen, der sofort seine Arbeit beginnt, sobald man ihn anklickt! Dabei handelt es sich um selbst ausführende Programme, die an persönliche oder abgelegte Unternehmensdaten gelangen wollen.

## WORAN ERKENNT IHR SOLCHE MAILS?

Es ist für den Laien nicht immer einfach, gut von schlecht oder gar böse zu unterscheiden. Merkmale für Spam, Fake und bösartigen Mails können folgende sein:

1. **Keine persönliche Anrede**
   Der Absender kennt nur eine Mailadresse, die er irgendwo im Internet oder nach erfolgreichen Einbrüchen gescannt hat. Er kennt aber nicht die Person, die diese Adresse empfängt.

2. **Nicht auf Deutsch verfasst**
   International aktive Versender kennen mitunter nicht einmal die Sprache des Empfängers.

3. **Merkwürdig übersetzt,**
   wenn die Sprache des Empfängers bekannt ist, aber mit falschem Deutsch geschrieben wurde und stümperhaft übersetzt ist.

4. **Fake Design**
   Raffinierter wird es, wenn eine Copyright-Identität vorgegaukelt wird. Mit HTML-Design einer Webseite oder den Farben des eigenen Vereins. Was unter Webseiten ebenfalls bekannt ist, findet auch für Mails statt. Tägliche Beispiele gehen bei uns mit dem Design von Banken, paypal und Versandt-Diensten ein. Davon sollte sich niemand beeindrucken lassen!
   **Auch unter diesen Erscheinungen sind die Merkmale 1-3 vorrangig zu beachten!**

5. **Mail-Absender mit vertrauter Domain nach dem @-Zeichen**
   Wer eine eigene Domain oder Webseite besitzt, hat es auch schon erlebt, dass er Spam mit eigenem Domain-

Namen erhält (in unserem Fall, Mails mit @dfeug.de). Das muss den Domainbesitzern in den meisten Fällen nicht beunruhigen. Der Spammer, der die E-Mail versendet, nutzt das sogenannte Mail Spoofing aus. Dabei wird die eigene E-Mail-Adresse als gefälschter Absender verwendet.
In manchen E-Mail-Programmen ist es möglich, einen anderen E-Mail-Absender als die eigentliche E-Mail-Adresse einzutragen – dies kann leider auch zu kriminellen Zwecken verwendet werden.
Eine Antwort würde ein Versender mit diesem Trick nicht erhalten und tarnt diese Mailadressen vorzugsweise mit noreply vor dem @-Zeichen (keine Antwort möglich).
Es geht den Absendern auch nicht um Antworten auf ihre Mails. Die Gefahr lauert immer in den Verlinkungen im Body dieser Mails.
Der wahre Absender oder zumindest die tatsächliche Mailadresse zeigt sich im Mail-Header der Mailprogramme. Leider mit etwas Aufwand und Wissen aus der code-Sprache.

6. **Emotet**
   Die gefährlichste Verbreitung ging in der Vergangenheit bereits vor dem Ukraine-Krieg von einem Virus namens Emotet aus. Dieser Virus ist seit 2014 bekannt und wird immer raffinierter und gefährlicher. Er verbreitet sich von infizierten Rechnern. Antwortet mit alten Inhalten eines Mailpostfachs dieser Rechner und schreibt Adressen aus dem Adressbuch an, die auf diese Inhalte reagieren könnten, weil sie aus einem alten Mailverkehr stammen. Damit suggeriert er Vertraulichkeit und infiziert bei Empfängern, die darauf hereinfallen, weitere Rechner.
   Er verweilt dort einige Zeit, bevor er zuschlägt und die Inhalte der Empfänger nach Belieben verschlüsselt, sodass man nicht mehr an eigene Daten herankommt.
   Emotet war bedauerlicherweise im Jahr 2019 auch auf Rechnern von DFeuG-Mitgliedern zu finden und ist noch nicht komplett eliminiert. Alle Virusprogramme haben sich inzwischen auf Emotet eingestellt und bieten einen guten Schutz, so wie auch der Virusschutz, den wir auf unseren eigenen Rechnern installieren. Offensichtlich existieren aber noch Rechner, die aus dieser Zeit gestartet werden und unseren Virusschutz nicht installiert haben. Dann tauchen diese Antworten mit zitiertem altem Text wieder auf.

Am Ende der Aufzählung ist es bedauerlicherweise etwas technisch geworden. Das Prinzip oder die Methoden dürften aber hoffentlich klar geworden sein.
Zum Emotet-Virus kann ich noch eine Audiospur nachreichen, die am 22.03.23 auf RadioEINS gelaufen ist.

## Oberstes Gebot ist, keine unnötige Neugier entwickeln. SAFTY FIRST!

## DIE RICHTIGE VORGEHENSWEISE

- Nicht antworten
- Keine Verlinkungen anklicken!
- Keine Anlagen oder Bilder öffnen
- Niemals weiterleiten!
- Löschen

## EINFACH LÖSCHEN!

Damit kann weiterer Schaden verhindert werden, wenn eine Spam-Mail bösartige Inhalte oder Verlinkungen enthält. Sollte man sich nicht sicher sein, hilft auch mal ein Anruf beim vermeintlich bekannten Absender, den man fragen kann, ob diese Mail von ihm an dem Tag des Erhalts ausgegangen ist.

## UMGANG MIT ADRESSEN DER DFEUG

Unsere Mailadressen sollten nicht für Werbung oder Newsletter weitergegeben werden. Wenn wir für die DFeuG etwas bestellen müssen, sollten wir darauf achten, dass das Häkchen für weitere Werbung oder Newsletter entfernt wird. Wir wissen nie, wie sicher unsere Daten bei diesen Unternehmen geschützt sind.

Geraten unsere internen Mails erst einmal in den Umlauf, haben wir selbst die Verbreitung nicht mehr unter Kontrolle. Es findet immer ein Datenmissbrauch statt, wenn ihr Werbung oder Newsletter von jemanden erhaltet, die ihr nicht angefordert habt. Jeder Newsletter muss irgendwo innerhalb der Nachricht mit einem Link versehen sein, um ihn abbestellen zu können. Oft sehr klein, mit schwachem Kontrast.

Aber Vorsicht! Bei Mails, die Euch unbekannt vorkommen, kann es sein, dass auch diese Verlinkungen bösartig ist!

Bleibt sicher im Netz und schützt Eure und unsere Daten.

*Seele*

--
Thomas Rohde-Seelbinder
DFeuG IT / Website
https://dfeug.de/it

E-Mail: it@dfeug.de

## VERLINKUNGEN ZU DIESEM THEMA

Was ist ein Virus und welche Auswirkungen kann ein Befall haben? AVAST-Info
https://www.avast.com/de-de/c-computer-virus

BSI zu EMOTET
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Sonderfall-Emotet/sonderfall-emotet_node.html

BSI-Archiv "Sicher informiert"
https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Buerger-CERT-Abos/Newsletter-Sicher-informiert/newsletter-sicher-informiert_node.html

Verbraucherzentrale, Mail-Header richtig auslesen
https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/so-lesen-sie-den-mailheader-6077