

Spoofting-Mails von der Adresse abtIV@fachlehrerausbildung....

Seit einiger Zeit sind E-Mails im Umlauf, deren Absenderadresse gefälscht ist. Der IT-Verlag „Heise Security“ weist darauf bereits seit Mitte September hin:

<https://www.heise.de/security/meldung/Achtung-Aktuelle-Spam-Mails-faelschen-Absender-von-Mitarbeitern-3834782.html>

Die E-Mails sind besonders gefährlich, da sie scheinbar von anderen Kollegen oder bekannten Adressen kommen.

ACHTUNG:

- Die angezeigten Absender dieser E-Mails sind gefälscht!
- Die angegebenen Links verweisen auf ein Dokument, das einen Computervirus enthält, d.h. sobald Sie das Dokument öffnen, gelangt Schadsoftware auf Ihren PC.

Bitte beachten Sie unbedingt die folgenden drei Hinweise:

1. Prüfen Sie, wer Ihnen die E-Mail geschickt hat!

Schauen Sie bei jeder E-Mail genau hin, von welcher E-Mail-Adresse sie verschickt wurde. Der in der E-Mail angezeigte Name stimmt nicht immer mit der tatsächlichen Absenderadresse überein.

Beispiel:

Im Kopfteil der E-Mail steht: Elfriede Musterfrau <heinz.datenklaue@spamversand.com>

Das bedeutet: Nicht(!) Elfriede Musterfrau, sondern der in Klammern angegebene Heinz Datenklaus (oder jemand, der die Adresse von Heinz Datenklaus missbräuchlich nutzt) hat die E-Mail geschrieben.

2. Seien Sie vorsichtig bei Links zu anderen Webseiten oder bei angehängten Dateien!

Klicken Sie in E-Mails nur dann auf angegebene Links, wenn Sie ganz sicher sind, dass die E-Mail vom angegebenen Absender kommt. Öffnen Sie Anlagen von E-Mails ebenfalls nur dann, wenn Sie sich über den Absender im Klaren sind.

3. Bevor Sie einen Link anklicken oder einen Dateianhang öffnen, klären Sie im Zweifelsfall telefonisch mit dem vermeintlichen Absender, ob er Ihnen die E-Mail tatsächlich geschickt hat.

Mit freundlichen Grüßen

Gez. Norbert Loos
Leiter des Staatsinstitutes IV