Informationen zu Phishing-E-Mails

hmt
Hochschule für Musik
und Theater Rostock

Was ist Phishing?

Phishing ist eine Betrugsmethode im Internet. Beim Phishing versuchen die Angreifenden an personenbezogene Daten und insbesondere Passwörter zu gelangen. Häufiges Ziel von Phishing sind die Zugangsdaten für E-Mail-Konten als „Türöffner“ zum Online-Leben der Betroffenen (Social-Media-Accounts, Accounts zum Online-Shopping, Banking-Zugänge etc.).

Woran erkenne ich eine Phishing-E-Mail?

Treffen ein oder mehrere der folgenden Merkmale auf eine E-Mail, die Sie erhalten haben zu, handelt es sich wahrscheinlich um eine Phishing-E-Mail (Beispiele in Anführungszeichen):

- unbekannte E-Mail-Adresse der absendenden Person
- unpersönliche Anrede ohne den Namen zu nennen: „Hallo …@hmt-rostock.de“
- Vorgeben einer erhöhten Dringlichkeit: „Wenn Ihr E-Mail-Konto innerhalb der nächsten 24 Stunden nicht überprüft wird, …“
- Drohungen: „Andernfalls wird Ihr Konto aus dem System entfernt.“
- ein oder mehrere Links, die nicht von der hmt Rostock stammen
  Links der hmt Rostock enden immer mit hmt-rostock.de:
  „https://service.hmt-rostock.de“
- eine Aufforderung persönliche Daten und Passwörter preiszugeben
  Weder die hmt Rostock noch der die Firma Gecko als IT-Dienstleister der hmt werden jemals dazu auffordern, ein Passwort freizugeben.
- sprachliche Fehler
- falsch oder gar nicht dargestellte Umlaute („ä“, „ö“, „ü“)

Wie verhalte ich mich, wenn ich eine Phishing-E-Mail erhalten habe?

- Ignorieren Sie die E-Mail und löschen Sie diese.
- Klicken Sie keinerlei Links an.
- Sollten Sie versehentlich dennoch einen Link angeklickt haben, schließen Sie ihren Internetbrowser umgehend.
- Geben Sie niemals Ihr Passwort preis.
  Technischer Support ist ohne diese Information möglich.
- Öffnen Sie keine Anhänge, die Sie nicht erwarten oder zuordnen können. Besonders gefährlich können Dateien folgender Formate sein: *.zip, *.doc, *.docx,*.xls, *.xlsx

Sollten Sie unsicher sein, ob es sich um eine Phishing-Mail handelt
(z. B. wenn die E-Mail-Adresse der absendenden Person von der hmt zu sein scheint)

- Prüfen Sie, ob der Absender oder der Text der E-Mail in der Sammlung von Phishing-E-Mails bereits aufgeführt ist.
- Wenden Sie sich an die Ansprechperson der hmt und ignorieren Sie die E-Mail zunächst.

Wie verhalte ich mich, wenn ich versehentlich personenbezogene Daten Preis gegeben habe?

Sollten Sie dennoch einmal personenbezogene Daten, wie das Passwort Ihres E-Mail-Accounts, preisgegeben haben:

- Ändern Sie umgehend Ihr Passwort. Nutzen Sie hierfür ausschließlich die gewohnte Weboberfläche unter https://exchange2013.hmt-rostock.de/.
- Informieren Sie darüber hinaus die Ansprechperson der hmt.