Gefälschte Helpdesk-E-Mails

English version below

Kurzfassung / Abstract

Es gibt zwei wesentliche Punkte, an denen Sie einen Phishing-Versuch erkennen können:

- Achten Sie genau auf die **Absender-Adresse** einer Mail und *nicht* auf den vorangesetzten *Absendernamen* - der lässt sich nämlich leicht fälschen!
- Bei Verlinkungen achten Sie genau auf die **Linkadresse**: Verweist diese nicht auf eine mit *https://xyz.hhu.de* beginnende Adresse, handelt es sich um eine Fälschung!

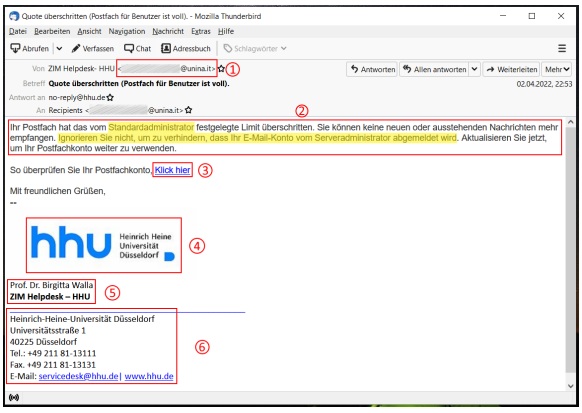
There are two main points by which you can recognize a phishing attempt:

- Pay close attention to the **sender address** of a mail and *not* to the prefixed *sender name* - because this can be easily faked!
- If links are embedded, pay close attention to the **link address**: If it does not refer to an address beginning with *https://xyz.hhu.de*, it is a fake!

Da immer wieder Phishing-Mails mit dem vermeintlichen Absender „Helpdesk“ verschickt werden, möchten wir hier einige Hinweise geben, wie Sie diese Fälschungen erkennen können:

- **Absendeadresse:** E-Mails des Helpdesk werden grundsätzlich immer von der offiziellen Adresse **helpdesk[at]hhu.de** verschickt! Beachten Sie aber bitte, dass sich E-Mail-Adressen auch fälschen lassen! Die (scheinbare) Absenderadresse allein ist also nicht zwingend aussagekräftig!
- **Betreffzeile:** E-Mails des Helpdesk enthalten grundsätzlich immer eine **Ticketnummer**, die dem Betreff vorangestellt ist!
- **Anrede:** Sie werden in E-Mails des Helpdesk grundsätzlich immer **namentlich angesprochen**!
- **Inhalt:** Der Helpdesk verschickt niemals E-Mails mit verdeckten Links! Vom Helpdesk verschickte Links verweisen grundsätzlich immer nur auf universitäre Seiten, deren Adresse auf „hhu.de“ oder „uni-duesseldorf.de“ endet! Ausnahmen sind die externen Dienste „Sciebo“ (sciebo.de) und Webex (webex.com). Über den Helpdesk werden niemals Rundmails verschickt!
- **Bildelemente:** Helpdesk-E-Mails enthalten niemals eingebettete Bildelemente (z.B. das HHU-Logo)!
- **Signatur:** E-Mails des Helpdesk geben immer den Namen der Mitarbeiterin/des Mitarbeiters an, welche/r die E-Mail verschickt hat! Die Signatur enthält immer die offiziellen Kontaktdaten des Helpdesk, wie sie auch auf der Homepage der HHU und des ZIM veröffentlicht sind.

Beispiel für eine gefälschte Helpdesk-Mail:



1. Falsche Absenderadresse (in diesem Beispiel nicht einmal eine HHU-Adresse!). Wenn Ihr E-Mail-Programm nur den Absendernamen, nicht aber die Adresse anzeigt, klicken Sie den Absendernamen an bzw. gehen Sie mit dem Mauszeiger darauf, dann wird die Adresse angezeigt.
2. Der Text enthält ungebräuchliche Begriffe (hier "Standardadministrator") und ist in fehlerhaftem Deutsch verfasst (hier: "Ignorieren Sie nicht, um zu verhindern, dass Ihr E-Mail-Konto vom Serveradministrator abgemeldet wird").
3. Verdeckter Link, der auf eine Seite verlinkt, die in diesem Beispiel wie folgt aussieht (aus Sicherheitsgründen verändert): https://providername.xy/servicedesk.hhu.de. In diesem Fall

Support

Bei Rückfragen oder Unsicherheiten im Zusammenhang mit Spam oder Phishing-E-Mails kontaktieren Sie bitte:

ZIM-Helpdesk

Tel.: +49 211 81-10111

E-Mail: helpdesk@hhu.de

Gebäude 25.41, Raum 00.53

Servicezeiten: Mo.-Fr. 8.30-18 Uhr

Melden von IT-Sicherheitsvorfällen

CERT (Computer Emergency Response Team)

E-Mail: cert@hhu.de

Weitere Sicherheitshinweise und Informationen

Sicherheitshinweise

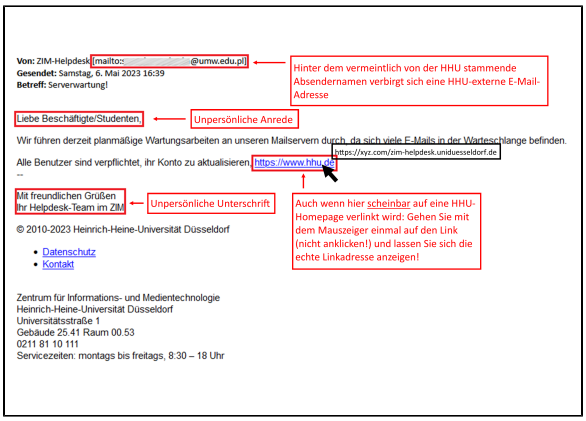
CEO-Fraud-E-Mails

Melden von Spam- und Phishingmails

Blacklisting

muss man sehr genau hinschauen, um zu sehen, dass "servicedesk.hhu.de" nicht die eigentliche Zielseite des Link ist, sondern "providername.xy".
4. Helpdesk-E-Mails enthalten keine Bildelemente.
5. Die Signatur enthält einen erfundenen Namen mit einem für einen IT-Helpdesk untypischen und unwahrscheinlichen akademischen Titel (hier: "Prof. Dr.").
6. Die Signatur enthält zwar den Namen der Universität, aber nicht der Einrichtung (Zentrum für Informations- und Medientechnologie/ZIM). Es werden eine erfundene Telefon-, Faxnummer und E-Mail-Adresse angegeben, die nicht mit den auf den offiziellen Kanälen (HHU-/ZIM-Homepage) veröffentlichten Kontaktdaten übereinstimmen.

Aktuell beobachten wir auch auf den ersten Blick deutlich authentischer wirkende Phishing-Mails:



Bei Zweifeln an der Echtheit einer vermeintlich vom Helpdesk kommenden E-Mail fragen Sie bitte beim Helpdesk über die offiziellen Supportkanäle nach: www.zim.hhu.de/helpdesk

---

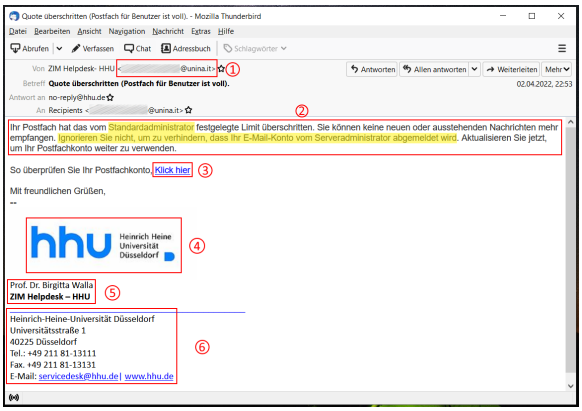
English Version

Fake e-mails from the Helpdesk

Since phishing e-mails with the supposed sender "Helpdesk" are sent out again and again, we would like to give you some tips here on how to recognise these fakes:

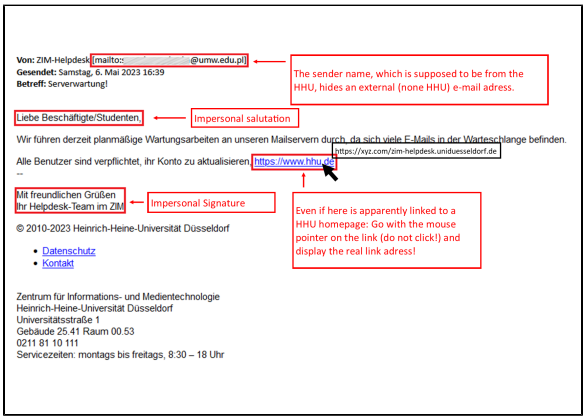
- **Sending address:** Helpdesk e-mails are always sent from the official address **helpdesk[at]hhu.de**! Please note, however, that e-mail addresses can also be faked! The (apparent) sender address alone is therefore not necessarily meaningful!
- **Subject line:** Emails from the Helpdesk always contain a **ticket number** that precedes the subject!
- **Salutation:** You will always be **addressed by name** in Helpdesk e-mails!
- **Content:** The Helpdesk never sends e-mails with hidden links! As a matter of principle, links sent by the Helpdesk always refer only to university pages whose address ends in "hhu.de" or "uni-duesseldorf.de"! Exceptions are the external services "Sciebo" (sciebo.de) and Webex (webex.com). Circular e-mails are never sent via the Helpdesk!
- **Image elements:** Helpdesk emails never contain embedded image elements (e.g. the HHU logo)!
- **Signature:** E-mails from the Helpdesk always indicate the name of the staff member who sent the e-mail! The signature always contains the official contact details of the Helpdesk, as they are also published on the homepage of HHU and ZIM.

Example of a forged helpdesk e-mail:



1. Wrong sender address (in this example not even a HHU address!). If your e-mail programme only displays the sender's name but not the address, click on the sender's name or move the mouse pointer over it and the address will be displayed.
2. The text contains uncommon terms (here "default administrator") and is written in incorrect German (here: "Do not ignore to prevent your e-mail account from being logged off by the server administrator").
3. Hidden link that links to a page that looks like the following in this example (modified for security reasons): https://providername.xy/servicedesk.hhu.de. In this case, you have to look very closely to see that "servicedesk.hhu.de" is not the actual target page of the link, but "providername.xy".
4. Helpdesk e-mails do not contain any picture elements.
5. The signature contains an invented name with an untypical and unlikely academic title for an IT helpdesk (here: "Prof. Dr.").
6. The signature contains the name of the university, but not of the institution (Centre for Information and Media Technology/ZIM). A fictitious telephone number, fax number and e-mail address are given, which do not match the contact details published on the official channels (HHU/ZIM homepage).

Currently, we are also observing phishing e-mails that appear much more authentic at first glance:



If in doubt about the authenticity of an e-mail supposedly coming from the helpdesk, please ask the helpdesk via the official support channels: www.zim.hhu.de/helpdesk