Sicherheitshinweise

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!

Inhalt / Content

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

Gefälschte Helpdesk-E-Mails

Spear-Phishing

CEO-Fraud-E-Mails

Melden von Spam- und Phishingmails

Blacklisting

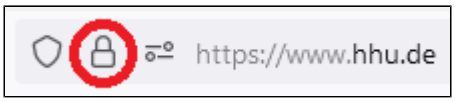
Was ist Phishing?

- **Phishing** ist der Versuch, Nutzerinnen und Nutzer von Online-Diensten per E-Mail zur Preisgabe ihrer Zugangsdaten (Kennung, Passwort) zu verleiten.
- Phishing-Mails **geben vor, von einer offiziellen Einrichtung der Universität zu stammen** (insbesondere von der Universitäts-IT der HHU, dem "Zentrum für Informations- und Medientechnologie" (ZIM)).
- Phishing-Mails fordern unter einem Vorwand (Androhung einer Account-Sperrung, angeblich voller Postfach-Speicherplatz oder ähnliches) dazu auf, sich über eine **verlinkte Homepage** mit den Zugangsdaten (Unikennung, Passwort) anzumelden.

Wie kann ich mich vor Phishing-Mails schützen?

- **Nur auf HHU-Seiten einloggen:** Melden Sie sich mit Ihrer Uni-Kennung und Ihrem Passwort nur auf Webseiten an, die von Ihrem Browser als sicher erkannt werden (mit einem geschlossenen Schloss gekennzeichnet). In der Adresszeile muss ein URL stehen, der mit *https://xyz.hhu.de* bzw. *https://www.xyz.hhu.de* beginnt.

  Sichere Homepages erkennt man am Schlosssymbol in der URL-Zeile:

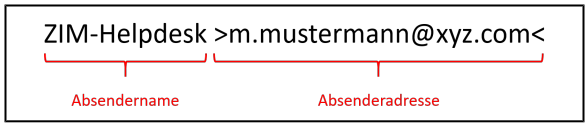


- **Lesezeichen verwenden:** Wenn Sie auf einen HHU-Online-Dienst zugreifen möchten, dessen genaue Adresse Sie nicht wissen, gehen Sie im Zweifelsfall zunächst auf die Startseite der HHU **www.hhu.de** und klicken Sie sich dort über die Verlinkungen zum gewünschten Dienst durch. Setzen Sie anschließend in Ihrem Browser ein Lesezeichen für die Adresse. Bei Links in E-Mails oder die Sie über eine Suchmaschine gefunden haben, schauen Sie genau hin, ob diese auf eine HHU-Homepage führen!
- **Misstrauisch sein:** Weder das ZIM noch andere Einrichtungen der HHU werden Sie per Mail auffordern, Ihre Zugangsdaten auf einer verlinkten Homepage einzugeben, um Ihren Account zu "bestätigen" oder zu "erneuern".
- **Auf Formulierungen/Ausdrücke achten:** Seien Sie vor allem vorsichtig bei Mails, die sprachlich „seltsam“ wirken oder Namen und Funktionsbezeichnungen enthalten, die an der HHU nicht verwendet werden – bedenken Sie aber auch, dass Phishing-Mails korrekt formuliert und mit täuschend echt wirkenden Signaturen, Logos und Absenderangaben ausgestattet sein können!
- **Helpdesk fragen:** Bei Zweifeln an der Echtheit einer vermeintlich von offiziellen HHU-Einrichtungen verschickten E-Mail fragen Sie bitte den Helpdesk des ZIM um Rat. Die Kontaktdaten finden Sie oben auf dieser Seite.

So erkennen Sie Phishing-Mails

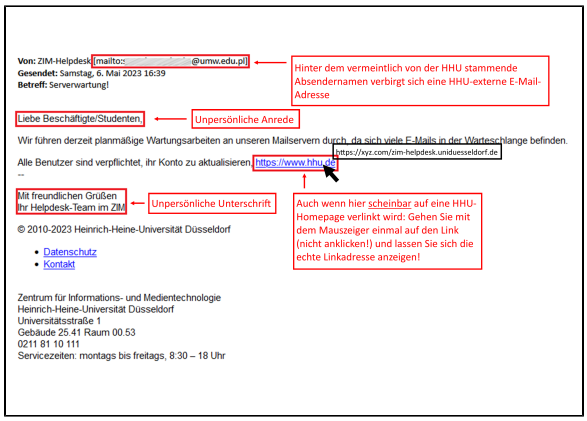
- **Absender-Adresse:** Die Absenderinformation in einer E-Mail besteht aus zwei Teilen: Dem *Absendernamen* und der *Absenderadresse*. Bei Phishing-Mails wird als Absendername meist eine HHU-Einrichtung angegeben (z.B. "ZIM-Helpdesk"). Schaut man dann genauer hin, sieht man, dass die Absenderadresse meist keine HHU-Adresse ist, sondern von einem fremden Anbieter kommt. In manchen Fällen werden allerdings auch kompromittierte persönliche HHU-Postfächer für den Versand solcher Mails verwendet - offizielle Mails der HHU werden allerdings nie von persönlichen E-Mail-Adressen aus verschickt! Wenn Ihnen (z.B. auf dem Handy) nur der Absendername angezeigt wird, klicken Sie diesen an - dann sehen Sie auch die Absenderadresse.

Beispiel für das Aussehen einer gefälschten E-Mail-Absenderinformation:

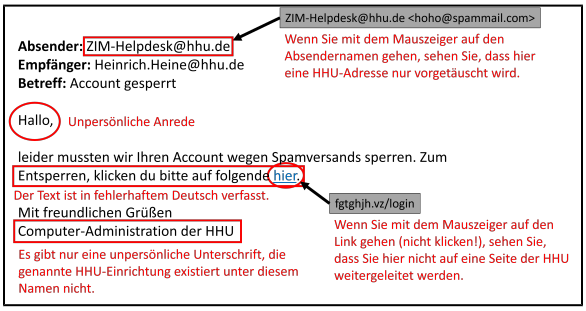


- **Anrede:** Meist keine oder nur unpersönliche Anrede.
- **Unterschrift:** Meist unpersönliche Unterschrift (nur Nennung eines Institutionennamens).
- **Falsche Einrichtungsnamen:** In den Phishing-Mails werden z.T. Einrichtungen als Absender genannt, die es unter diesem Namen an der HHU gar nicht gibt (z.B. "IT-Administration der HHU", "ZIM-Servicedesk" oder ähnliches). In der Signatur werden Kontaktdaten angegeben, die nicht mit den offiziell veröffentlichten übereinstimmen.
- **Unpräziser Inhalt:** Allgemein gehaltene Informationen im Text, kein Bezug zum konkreten Account der Nutzerin/des Nutzers.
- **Rechtschreibe- und Grammatikfehler:** Der Text weißt auffällige Fehler in Rechtschreibung und Satzbau auf.
- **Fremdsprache:** Der Text ist in einer für den Absender untypischen Fremdsprache verfasst.
- **Psychischer Druck:** Es wird psychischer Druck aufgebaut und eine hohe Dringlichkeit suggeriert (z.B. "es muss *sofort* gehandelt werden, sonst wird Ihr Account *gesperrt*").
- **Links:** Phishing-Mails enthalten immer einen Link, der entweder hinter einem Fließtext (z.B. "Hier klicken") versteckt ist oder einen vermeintlichen HHU-Link enthält.
    - Wenn Sie mit dem Mauszeiger auf den Link gehen (nicht anklicken!) sehen Sie, ob der Link tatsächlich auf eine Homepage verlinkt, die mit *https://xyz.hhu.de* bzw. *https://www.xyz.hhu.de* beginnt.
    - Homepages mit Adressen wie z.B. *http://abc.com/zim.hhu.de* sind dagegen Fälschungen!

Beispiel für eine (auf den ersten Blick durchaus authentisch wirkende) Phishing-Mail:



Beispiel für eine eher plumpe Phishing-Mail:



Umgang mit Phishing-Mails

- **Keine unbekannten/ungewöhnliche E-Mail-Anhänge öffnen:** Öffnen Sie niemals an E-Mails angehängte Dateien (insbesondere Office- und PDF-Dokumente) und klicken Sie niemals auf Links in E-Mails von Ihnen unbekannten Personen!
- Öffnen Sie niemals an E-Mails angehängte Dateien und klicken Sie niemals auf Links in E-Mails von Ihnen bekannten Personen, wenn der angebliche Inhalt der E-Mail für die absendende Person ungewöhnlich ist! Wenn Ihnen eine bekannte Person z. B. normalerweise keine Rechnungen schickt, der E-Mail aber eine Datei mit dem Titel „Rechnung“ anhängt, ist äußerste Vorsicht geboten!
- **Keine Makros aktivieren:** Aktivieren Sie beim Öffnen von per E-Mail zugesandten Dateien kein e Makros (dies betrifft v. a. Microsoft Office-Dokumente wie *Word* und *Excel*)!

> Aus Sicherheitsgründen ist der **Empfang wie auch der Versand von Dateianhängen im alten Microsoft-Office-Format (.doc, .xml, .ppt)** per E-Mail seit Dezember 2019 an der HHU verboten. E-Mails mit entsprechenden Anhängen werden vom Spamfilter zurückgewiesen!

- **Zugangsdaten niemals auf verlinkten Seiten eingeben:** Das Zentrum für Informations- und Medientechnologie (ZIM) oder andere Universitätseinrichtungen werden Sie niemals per E-Mail bitten, Ihre persönlichen Zugangsdaten (Unikennung, Passwort) auf einer verlinkten Internetseite einzugeben! Lassen Sie sich hierzu auch nicht durch Androhungen von Konto-Sperrungen o. ä. verleiten!
- **Phishing-Mails melden:** Nutzer:innen des E-Mail-Portals *Roundcube* und *Exchange* schicken Spam und Phishing-Mails bitte als Dateianhang (EML-Datei) an die Meldeadresse spamreport@hhu.de. (s. hierzu https://wiki.hhu.de/x/CoiQAg, hier unter "Falsch klassifizierte Mail" schauen).

Was tun, falls Sie trotzdem Opfer einer Phishing-Mail oder von Schadsoftware geworden sind?

Wenn Sie vermuten, dass Unbefugte sich Zugang zu Ihrem Universitätskonto und/oder Computer verschafft haben, ergreifen Sie sofort folgende Maßnahmen:

- **Sofort Passwort ändern:** Ändern Sie sofort auf der Seite https://idm.hhu.de/ Ihr Passwort *oder* informieren Sie den ZIM-Helpdesk, damit dort Ihr Passwort zurückgesetzt wird! Wenn Sie vermuten, dass Ihr Computer gehackt wurde, nutzen Sie für die Änderung des Passworts ein anderes Gerät!
- Falls Ihr Computer mit Schadsoftware infiziert wurde, müssen Sie auch die Passwörter aller von Ihnen genutzten Dienste ändern, auf die Sie von dem betroffenen Computer aus zugegriffen haben (z. B. private E-Mail-Konten, Online-Banking usw.)!
- **Sofort Netzzugang trennen:** Wenn Sie vermuten, dass Unbefugte Zugang zu Ihrem Computer erlangt haben, trennen Sie diesen sofort vom Internetzugang. Wenn Sie über ein LAN-Kabel mit dem Internet verbunden sind, ziehen Sie den LAN-Stecker, falls Sie ein WLAN benutzen, deaktivieren Sie die WLAN-Verbindung Ihres Gerätes!
- **Computer auf Schadsoftware scannen:** Überprüfen Sie den betroffenen Computer in jedem Fall mit einer Virenschutz-Software!
- **Betriebssystem neu installieren:** Wenn möglich, installieren Sie das Betriebssystem des betroffenen Computers neu!
- **Kontakte warnen:** Informieren Sie Ihre E-Mail-Kontakte über die Infektion Ihres Rechners, da für diese Personen jetzt eine erhöhte Gefahr besteht!

Bitte beachten Sie: Fallen einzelne HHU-Nutzerkonten durch den Versand von Spam- oder Phishing-E-Mails als kompromittiert auf, werden diese durch das ZIM sofort gesperrt! Eine gesonderte (Vor-) Warnung erfolgt nicht! Für die Entsperrung wenden Sie sich bitte an den ZIM-Helpdesk.

Vorbeugende Maßnahmen

- **Datensicherung:** Sichern Sie regelmäßig die Daten auf Ihrem Computer auf einem USB-Stick oder einer externen Festplatte!
- **Virenschutzsoftware verwenden:** Insbesondere bei Microsoft Windows-Computern: Verwenden Sie eine auf dem tagesaktuellen Stand befindliche Virenschutzsoftware (auf den Dienstrechnern der HHU sind solche Programme in der Regel bereits installiert)!
- **Updates installieren:** Halten Sie das Betriebssystem Ihres Computers und die darauf befindlichen Programme immer auf dem aktuellsten Stand!

English Version: Identify Phishing Emails

What is Phishing?

- **Phishing** is the attempt to trick users of online services into revealing their access data (ID, password) by email.
- Phishing emails **pretend to come from an official institution of the university** (in particular from HHU's university IT, the "Center for Information and Media Technology" (ZIM)).
- Phishing emails use a pretext (threat of account blocking, allegedly full mailbox storage space or similar) to ask users to log in via a **linked homepage** using their access data (unique identifier, password).

How can I protect myself from phishing emails?

- **Log in only on HHU pages:** Log in with your university ID and password only to websites that are recognized as secure by your browser (marked with a closed lock). The address line must contain a URL that begins with *https://xyz.hhu.de* or *https://www.xyz.hhu.de*.

  Secure Homepages can be recognized by the lock symbol in the URL line:

- **Use bookmarks:** When in doubt, if you want to access an HHU online service for which you do not know the exact address, first go to the HHU home page at www.hhu.de and click through the links to the desired service. Then bookmark the address in your browser. For links in e-mails or that you have found via a search engine, look carefully to see if they lead to an HHU home page!
- **Be suspicious:** Neither ZIM nor other HHU institutions will ask you by mail to enter your access data on a linked homepage in order to "confirm" or "renew" your account.
- **Pay attention to wording/expressions:** Be especially careful with mails that seem "strange" in terms of language or contain names and function designations that are not used at HHU - but also keep in mind that phishing mails can be correctly formulated and equipped with deceptively real-looking signatures, logos and sender information!

- **Ask the Helpdesk:** If in doubt about the authenticity of an e-mail supposedly sent by official HHU institutions, please ask the ZIM Helpdesk for advice. The contact details can be found at the top of this page.

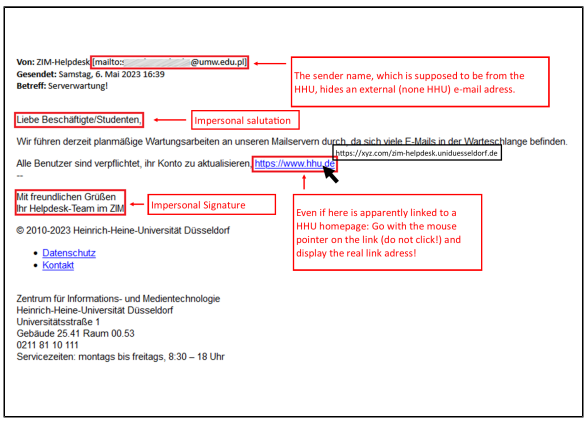
How to recognize Phishing emails

- **Sender address:** The sender information in an email consists of two parts: The sender name and the sender address. In phishing e-mails, the sender name is usually an HHU institution (e.g. "ZIM Helpdesk"). If you then take a closer look, you will see that the sender address is usually not an HHU address, but comes from a third-party provider. In some cases, however, compromised personal HHU mailboxes are also used to send such mails - official HHU mails are never sent from personal email addresses, however! If you are only shown the sender name (e.g. on your cell phone), click on it - then you will also see the sender address.

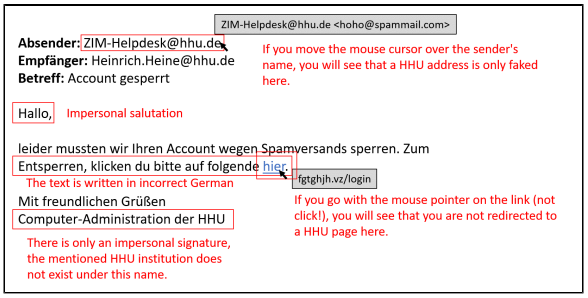
Example for a forged sender information:

- **Salutation:** Usually no salutation or only impersonal salutation
- **Signature:** Mostly impersonal signature (only mention of an institution name).
- **Incorrect institution names:** In the phishing e-mails, institutions are sometimes named as senders that do not even exist under this name at HHU (e.g. "IT-Administration of HHU", "ZIM-Servicedesk" or similar). In the signature, contact details are given that do not match the officially published ones.
- **Inaccurate content:** General information in the text, no reference to the user's specific account.
- **Spelling and grammatical errors:** The text has conspicuous errors in spelling and sentence structure.
- **Foreign language:** The text is written in a foreign language that is not typical for the sender.
- **Psychological pressure:** Psychological pressure is built up and a high degree of urgency is suggested (e.g. "action must be taken *immediately*, otherwise your account will be *blocked*").
- **Links:** Phishing emails always contain a link that is either hidden behind body text (e.g. "Click here") or contains a supposed HHU link.
    - If you move your mouse pointer over the link (don't click!) you can see if the link actually links to a homepage that starts with *https://xyz.hhu.de* or *https://www.xyz.hhu.de*.
    - Homepages with addresses like e.g. *http://abc.com/zim.hhu.de* are fakes!

Example of a (at first glance authentic-looking) phishing email:



Example of a rather clumsy phishing email:



Dealing with phishing emails

- **Do not open unknown/unusual e-mail attachments:** Never open files attached to e-mails (especially Office and PDF documents) and never click on links in emails from people you do not know!
- Never open files attached to emails and never click on links in emails from people you know if the alleged content of the e-mail is unusual for the person sending it! For example, if a person you know does not normally send you invoices, but attaches a file titled "Invoice" to the e-mail, exercise extreme caution!
- **Do not activate macros:** Do not activate macros when opening files sent by e-mail (this applies especially to Microsoft Office documents such as *Word* and *Excel*)!

> For security reasons, **receiving as well as sending file attachments in the old Microsoft Office format (.doc, .xml, .ppt)** via email is prohibited at HHU since December 2019. Emails with corresponding attachments will be rejected by the spam filter!

- **Never enter access data on linked pages:** The Center for Information and Media Technology (ZIM) or other university institutions will never ask you by e-mail to enter your personal access data (university ID, password) on a linked website! Do not be tempted to do so by threats of account blocking or similar!
- **Report phishing mails:** Users of the Roundcube e-mail portal and Exchange e-mail portal should send spam and phishing emails as file attachments (EML file) to the reporting address spamreport@hhu.de. (see https://wiki.hhu.de/x/CoiQAg, look here under "Falsch klassifizierte Mail").

What to do if you still became a victim of a phishing email or malware?

If you suspect that unauthorized persons have gained access to your University account and/or computer, take the following actions immediately:

- **Change password immediately:** Immediately change your password on the page https://idm.hhu.de/ *or* inform the ZIM Helpdesk to reset your password there! If you suspect that your computer has been hacked, use another device to change your password!
- If your computer has been infected with malware, you must also change the passwords of all services you use and have accessed from the affected computer (e.g. private email accounts, online banking, etc.)!
- **Disconnect network access immediately:** If you suspect that unauthorized persons have gained access to your computer, disconnect it from the Internet access immediately. If you are connected to the Internet via a LAN cable, disconnect the LAN plug, if you are using a WLAN, deactivate the WLAN connection of your device!
- **Scan computer for malware:** In any case, check the affected computer with antivirus software!
- **Reinstall the operating system:** If possible, reinstall the operating system of the affected computer!
- **Warn contacts:** Inform your e-mail contacts that your computer has been infected, as these people are now at increased risk!

Please note: If individual HHU user accounts are found to be compromised through the sending of spam or phishing e-mails, they will be blocked immediately by the ZIM! A separate (pre-)warning is not given! For unblocking, please contact the ZIM Helpdesk.

Preventive measures

- **Data backup:** Regularly back up the data on your computer on a USB stick or an external hard drive!
- **Use virus protection software:** Especially with Microsoft Windows computers: Use an up-to-date virus protection software (such programs are usually already installed on the HHU company computers)!
- **Install updates:** Always keep your computer's operating system and the programs on it up to date!