Sicherheitshinweise für den Umgang mit Spam und Phishing-E-Mails

In jüngster Zeit hat es vermehrt Spam- und Phishing-Attacken auf E-Mail-Postfächer der Heinrich-Heine-Universität gegeben, in denen insbesondere versucht wurde, durch gefälschte E-Mails Nutzer der HHU-IT-Services zum Verrat Ihrer Zugangsdaten (Unikennung, Passworte) zu verleiten oder über an die Mails angehängte Dateien und Links Schadsoftware zu installieren. Im Folgenden möchten wir Ihnen einige Hinweise geben, wie Sie derartige Spam-E-Mails erkennen und mit diesen umgehen sollten. Weiterhin finden Sie hier Hinweise, wie Sie vorgehen müssen, falls Sie auf eine Spam- und Phishing-E-Mail hereingefallen sind und Ihre Zugangsdaten preisgegeben haben.

Spam: Bei Spam-E-Mails handelt es sich um unverlangt zugesandte E-Mails, meist mit werbendem Inhalt, sie können aber auch Drohungen enthalten.

Phishing: Mit Phishing-Mails versuchen Kriminelle an die Zugangsdaten von Computernutzern zu gelangen und so in Computersysteme insbesondere von Unternehmen, Behörden und auch Universitäten einzudringen, um dort zu spionieren oder die Systeme zu sabotieren.

Spoofing: Bei Spoofing handelt es sich um das Vortäuschen einer fremden Identität. Genauso wie auf einem Briefumschlag eine gefälschte Absenderanschrift stehen kann, können auch auch bei Mails fremde Absenderadressen vorgetäuscht werden. So können Angreifer sich beispielsweise als Vorgesetzte der Empfänger ausgeben.

Bei Rückfragen oder Unsicherheiten im Zusammenhang mit Spam oder Phishing-E-Mails kontaktieren Sie bitte den ZIM-Helpdesk (Tel. 0211-81 10111, E-Mail: helpdesk@hhu.de, Gebäude 25.41, Raum 00.53, Servicezeiten: Mo.-Fr. 8.30-18 Uhr).

Wie schütze ich mich vor Phishing-Mails

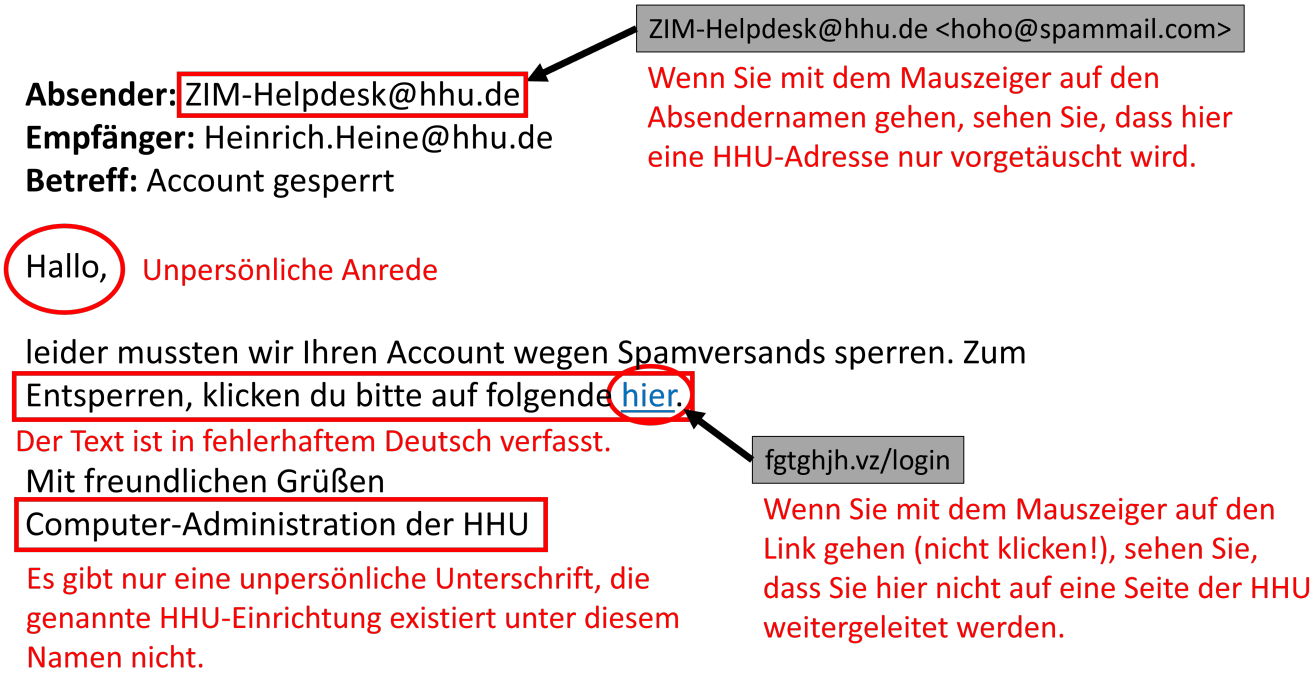
1. Melden Sie sich mit Ihrer Uni-Kennung und Ihrem Passwort nur auf Webseiten an, die von Ihrem Browser als sicher erkannt werden (mit einem geschlossenen Schloss gekennzeichnet). In der Adresszeile muss ein URL stehen, der mit „https://XXX.hhu.de/“ (oder „https://XXX.uni-duesseldorf.de/“) beginnt, wobei XXX für einen Servernamen steht.
2. Gehen Sie im Zweifel lieber über die HHU-Startseite (www.hhu.de) und von dort über klickbare Links zu den Services der HHU, anstatt einem Link in einer Mail oder den Ergebnissen einer Suchmaschine zu folgen. Speichern Sie dann ein Lesezeichen (Bookmark) der Seite, um sie künftig schnell wiederzufinden.
3. Vom ZIM oder anderen Stellen der HHU werden keine Mails versandt, die Sie auffordern, Ihr Passwort einzugeben, weil z.B. Ihr Mailaccount „bestätigt“ oder „erneuert“ werden muss. Seien Sie misstrauisch!
4. Wenn Ihnen eine empfangene Mail oder Kurznachricht dubios erscheint, fragen Sie beim Helpdesk des ZIM (Tel. +49-211-81-10111, Mail an helpdesk@hhu.de) nach, ob die Nachricht oder eine Webseite, auf die verwiesen wird, vertrauenswürdig sein kann.
5. 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!

So erkennen Sie Spam- und Phishing-Mails

Folgende Punkte können Indizien für Spam- bzw. Phishing-Mails sein. Bedenken Sie, dass oft sind nur wenige Merkmale vorhanden sind:

- Unpersönliche Anrede ohne Nennung Ihres Namens
- Unpersönliche Unterschrift (z. B. wenn nur mit einem Institutionenname unterschrieben wird) oder Unterschrift passt nicht zum Absendernamen
- Die als Absender genannte Einrichtung existiert unter diesem Namen nicht an der HHU (z.B. "ZIM-Servicedesk" anstatt "ZIM-Helpdesk", "IT-Administration der HHU" statt "ZIM")
- Allgemein gehaltene Formulierungen im Text
- Der Text enthält auffällige Rechtschreib- oder Satzbaufehler
- Der Text ist in einer für den Absender untypischen Fremdsprache verfasst
- Wenn Sie in Ihrem E-Mail-Programm mit der Maus auf den Absendernamen gehen, wird hinter einer angeblichen E-Mail-Adresse der HHU eine zweite, universitätsfremde E-Mail-Adresse angezeigt
- Sie werden aufgefordert, Zugangsdaten (Nutzerkennung, Passwörter) preiszugeben; der Text enthält dabei meist (verdeckte) Drohungen, z.B. dass Ihr E-Mail-Konto gesperrt wird/wurde und Sie sich für die Freischaltung auf einer verlinkten Internetseite anmelden müssen (s. hierzu unten). Die verlinkte Internet-Adresse (also z. B. www.uni-duesseldorf.de) ist dabei in der Regel in der E-Mail nicht direkt lesbar, sondern in einem Text versteckt.
- Sie werden mit vermeintlichen Videoaufnahmen oder Bildern erpresst und aufgefordert, Geld in Form von Bitcoins o. ä. zu bezahlen

Beispiel für das Aussehen einer Phishing-Mail:



Umgang mit Spam- und Phishing-Mails

1. 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!
2. Eine besondere Gefährdung geht von Dateien im alten Microsoft-Office-Format (mit den Endungen .doc, .xml und .ppt) aus (s. hierzu auch den Info-Kasten unten)!
3. 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!
4. Aktivieren Sie beim Öffnen von per E-Mail zugesandten Dateien keine Makros (dies betrifft v. a. Microsoft Office-Dokumente wie *Word* und *Excel*)!
5. 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, die nicht auf den Namen *uni-duesseldorf.de* oder *hhu.de* endet! Lassen Sie sich hierzu auch nicht durch Androhungen von Konto-Sperrungen o. ä. verleiten!
6. Nutzer des E-Mail-Portals *Roundcube* können auf https://roundcube.hhu.de Spam und Phishing-Mails in den Ordner „Spam“ verschieben und so den Spamfilter trainieren (s. auch https://wiki.hhu.de/display/HHU/Der+Spamfilter)
7. Nutzer des E-Mail-Portals *Exchange* schicken Spam und Phishing-Mails bitte als Dateianhang (EML-Datei) an die Meldeadresse spamreport@hhu.de. Schieben Sie die betreffende E-Mail hierfür im Webportal https://exchange.hhu.de einfach in eine neue E-Mail (s. hierzu https://wiki.hhu.de/display/HHU/Der+Spamfilter,hier unter "Methode 2" schauen)

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!

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:

1. Ändern Sie sofort auf der Seite https://idm.hhu.de/IDMProv 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!
2. 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!
3. Wenn möglich, installieren Sie das Betriebssystem des betroffenen Computers neu!
4. Überprüfen Sie den betroffenen Computer in jedem Fall mit einer Virenschutz-Software!
5. 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.)!
6. 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

- Sichern Sie regelmäßig die Daten auf Ihrem Computer auf einem USB-Stick oder einer externen Festplatte!
- 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)!
- Halten Sie das Betriebssystem Ihres Computers und die darauf befindlichen Programme immer auf dem aktuellsten Stand!