Phishing

Häufig gestellte Fragen (FAQ)

Was ist Phishing?

Unter dem Begriff **Phishing** (Neologismus von *fishing*, engl. für „Angeln“) versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Nutzers/einer Internet-Nutzerin zu gelangen und damit Identitätsdiebstahl zu begehen. *(Quelle: Wikipedia)*

Welcher Zweck wird mit Phishing verfolgt?

Mit Ihren Zugangsdaten zu einem geschützten System (etwa mit Ihrer Uni-Kennung und dem zugehörigen Passwort) können beispielsweise Werbemails (Spam) in Ihrem Namen verschickt, Ihre Daten in Online-Systemen wie LSF oder E-Learning-Plattformen manipuliert oder auf Ihre gespeicherten Daten zugegriffen werden, in schweren Fällen beispielsweise auf Forschungs- oder Personaldaten.

Wie schütze ich mich vor Phishing?

1. Melden Sie sich mit Ihrer Uni-Kennung und Ihrem Passwort nur auf Webseiten an, die von der HHU stammen. Diese beginnen stets mit „https://XXX.hhu.de/“ (oder „https://XXX.uni-duesseldorf.de/“), wobei XXX für einen Unterbereich („Subdomain“) steht. Vor der Adresse muss aus Sicherheitsgründen immer ein Vorhängeschloss-Piktogramm zu erkennen sein. Geben Sie Ihre Daten nicht auf unverschlüsselten Seiten ein.
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 niemals Mails versandt, die Sie auffordern, Ihr Passwort einzugeben, weil z.B. Ihr Mailaccount „bestätigt“ oder „erneuert“ werden muss.
4. Seien Sie misstrauisch! 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 zunehmend korrekt formuliert und mit täuschend echt wirkenden Signaturen, Logos und Absenderangaben ausgestattet sind!

Wenn es doch einmal passiert ist…

… und Sie den Verdacht haben, Sie könnten auf eine Phishing-Aktion hereingefallen sein, rufen Sie die Seite idm.hhu.de auf, klicken Sie auf „Passwort ändern“ und geben Sie Ihrer Uni-Kennung ein völlig neues, nicht zu erratendes Passwort. Benachrichtigen Sie anschließend den Helpdesk des ZIM oder melden den Vorfall an cert@hhu.de.

D. Lannert, ZIM, 01.10.2020