Zentrum für Informations- und Medientechnologie

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Heinrich-Heine-Universität Düsseldorf ZIM ✉ 40204 Düsseldorf

An
die Studierenden und Bediensteten
der Heinrich-Heine-Universität Düsseldorf

Task-Force Kommunikationsdienste

Julian Kippels M.Sc.

Telefon 0211 - 811 49 20
Telefax 0211 - 811 25 39
kippels@hhu.de

Düsseldorf, 16. Dezember 2013

Heinrich-Heine-Universität Düsseldorf
Universitätsstr. 1
40225 Düsseldorf
Gebäude 25.41
Ebene 01 Raum 25

www.zim.hhu.de

Betrifft: Phishing-Mails

Sehr geehrter Leserinnen und Leser,

in letzter Zeit kam es zu einer Häufung von Phishing-Angriffen auf unsere Universitätskennungen. Aus diesem Anlass möchten wir Sie vor den Gefahren dieser Angriffe warnen und Ihnen zeigen, mit welchen einfachen Maßnahmen Sie sich einfach gegen diese Angriffe schützen können.

Was sind Phishing-Mails und welche Gefahren entstehen daraus?
Mit Phishing-Mails versuchen Betrüger an Login-Informationen zu Universitätskonten zu kommen. Mit diesen Informationen können sie dann im harmlosesten (obwohl dies alles andere als harmlos ist) Fall Spam-Mails über die Universitätsserver verschicken und im schlimmsten Fall zum Beispiel unveröffentlichte Forschungsergebnisse stehlen.

Wie erkenne ich Phishing-Mails und was kann ich dagegen unternehmen?
In den meisten Fällen sind Phishing-Mails sehr einfach zu erkennen. Sie sind meist in sehr schlechtem deutsch geschrieben und kommen von Mailanbietern, die offensichtlich nicht von der Universität stammen, wie zum Beispiel:

- Michael.Ault-1@ou.edu ,
- be4study@mail.ubc.ca oder
- info@msn.net

Manche Phishing-Mails sind allerdings „besser" gestaltet und benutzen Namen wie „Office-Helpdesk", die tatsächlich existieren. Die „besten" Mails fälschen sogar die Absenderadresse, so dass sie allem Anschein nach wirklich von @hhu.de oder @uni-duesseldorf.de stammen. Ganz wenige Mails schaffen es sogar zudem noch offiziell erscheinende Signaturen, die manchmal von offiziellen Stellen kopiert sind, zu benutzen um noch seriöser zu wirken.

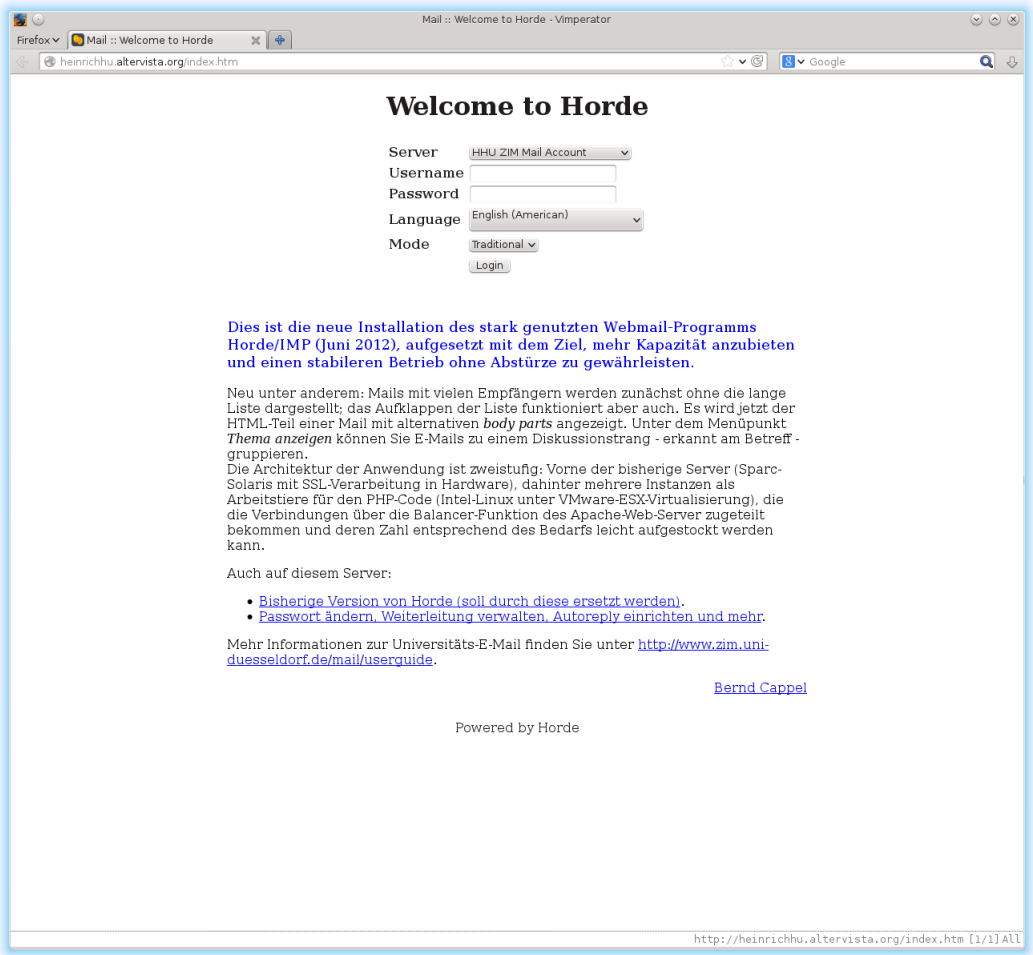
Allen Phishing-Mails ist gleich, dass Sie auf irgendeine Art und Weise Ihre Login-Daten übermitteln sollen. Sei es im Mailtext, oder auf einer

gefälschten Anmeldeseite. In den meisten Fällen wird jedoch eine gefälschte Seite benutzt. Solche Fälschungen sind in der Regel einfach zu erkennen:

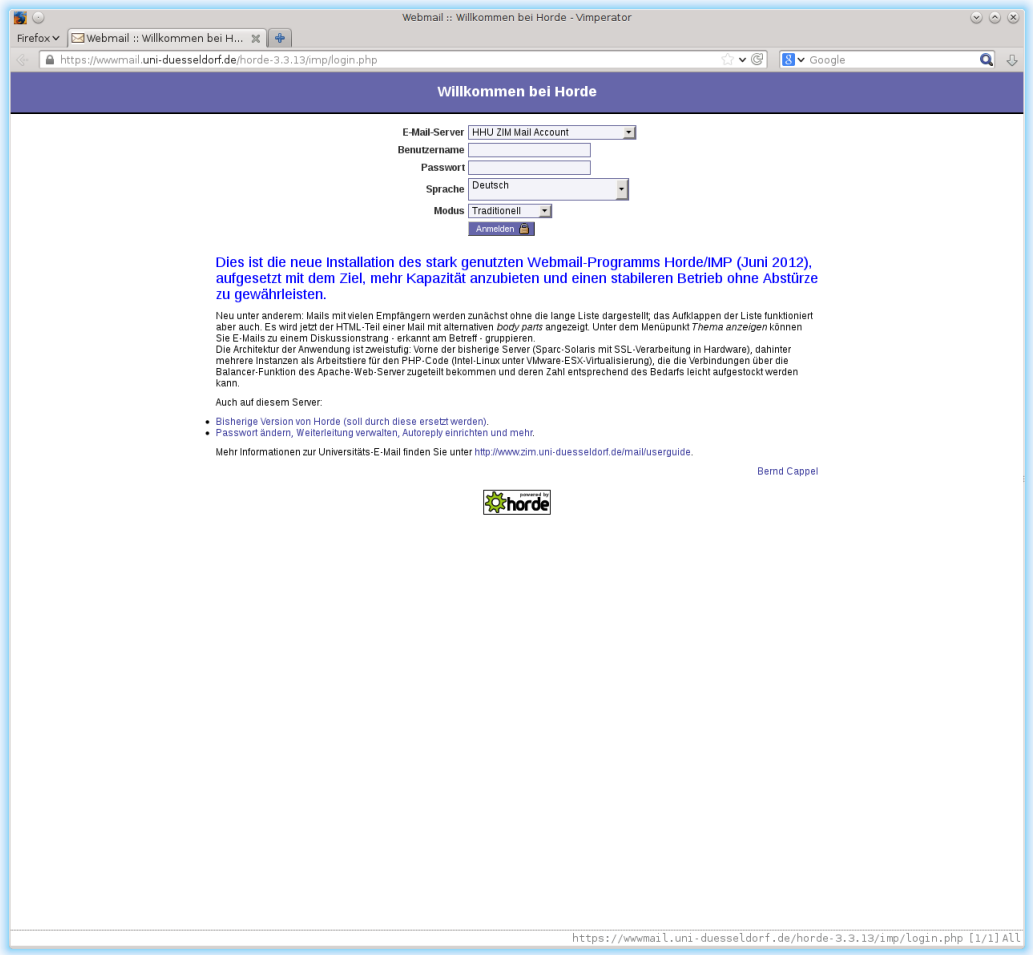
- Sie beinhalten URLs die nicht zur Uni gehören wie http://hhu.altervista.org/index.htm oder http://www.kentworks.com/PHPFORM/forms/form1.html .
- Sie benutzen keines der Webmail-Programme die von der Uni angeboten werden (Horde oder Convergence).
- Sie bauen die Login-Seiten der Webmail-Programme nach, aber benutzen falsche Farben.
- Keine der Seiten benutzt das sichere, verschlüsselte https, sondern immer nur unverschlüsseltes http.

Aber selbst wenn sie eine Mail, in perfektem deutsch, von einer definitiv aus der Uni stammenden Absenderadresse, mit einem Link auf einen Universtiätsseite über https bekommen sollten, gilt trotzdem folgende Faustregel: Die Universität wird sie **niemals** explizit nach Ihrem Passwort fragen. Solche Mails sind immer Phishing-Versuche!

Hier ist ein Beispiel für eine typische Phishingseite:



Zum Vergleich die korrekte Seite der Universität:



Bereits auf den ersten Blick ist zu erkennen, dass die Phisher einfach nur den Text und den Aufbau der Originalseite kopiert haben, aber nicht die Formatierung und die Farben übernommen haben. Wenn man noch genauer hinsieht, fallen einem gleich 3 Diskrepanzen in der Adresszeile des Browsers auf:

1. Die gefälschte Seite benutzt keine verschlüsselte Verbindung über https.
2. Die gefälschte Seite wird von einem fremden Server gehostet.
3. Die gefälschte Seite benutzt einen falschen Titel.

Was passiert, wenn Daten doch rausgegeben werden?
Wenn sie trotz allem Ihre Daten bei einer Phishing-Attacke freigegeben haben, sollten Sie so schnell wie möglich Ihr Passwort ändern. Falls Sie dies nicht tun und von uns ein Mißbrauch festgestellt wird, werden wir das Konto sofort kommentarlos sperren. Eine Entsperrung kann dann nur persönlich im Benutzerbüro, unter Vorlage von gültigen Ausweisdokumenten vorgenommen werden.

Mit freundlichen Grüßen
Ihr Mail-Team
Julian Kippels und Bernd Cappel