Der IT-Sicherheitsbeauftragte (CISO)

Dr. Christian Rank

UNIVERSITÄT PASSAU

Universität Passau · Rechenzentrum · D-94030 Passau

An alle Angehörigen
der Universität Passau

Telefon	0851 509-1838 0851 509-1801 (Sekretariat)
Telefax	0851 509-1802
e-mail	christian.rank@uni-passau.de
Zeichen	20151110_rs_phishing
Datum	10.11.2015

Phishing-Angriffe auf die Benutzerkennungen von Universitätsangehörigen

Sehr geehrte Damen, sehr geehrte Herren,

sog. **Phishing-Angriffe**, bei denen Kriminelle – leider z. T. durchaus mit Erfolg – versuchen, sich in den Besitz der Zugangsdaten der Benutzerkennungen von Universitätsangehörigen zu bringen, sind regelmäßig zu beobachten.

Im Rahmen eines derartigen Angriffs erhalten Sie eine mehr oder weniger authentisch wirkende E-Mail, in der Sie aufgefordert werden, entweder Ihre Zugangsdaten direkt an den Absender zu schicken oder diese auf einer Webseite, deren Link in der E-Mail angegeben ist, einzugeben.

Das ZIM¶ setzt zwar auf seinen Mailservern einen leistungsfähigen Spamfilter ein, der auch Phishing-Mails recht gut ausfiltert, in Einzelfällen werden jedoch solche unerwünschten E-Mails zugestellt, denn leider können automatisierte Spam- und Virenerkennungssysteme niemals eine Trefferquote von 100% erreichen.

Ende der letzten Woche erhielten viele Universitätsangehörige eine vorgeblich von einer Support-Stelle der Universität (Absender support@uni-passau.de) stammende Phishing-Mail mit dem Betreff "Konto-Update", die in sehr holprigem Deutsch verfasst war und daher bei den meisten betroffenen Benutzern berechtigtes Misstrauen erweckt hat. Nicht alle Phishing-Mails sind aber so schlecht gemacht.

Daher möchte ich Sie mit diesem Schreiben auf den richtigen Umgang mit derartigen Mails hinweisen.

Zunächst ist ausdrücklich festzustellen, **dass der Absenderangabe einer E-Mail grundsätzlich nicht vertraut werden kann**, weil Betrüger mit einfachen Mitteln den

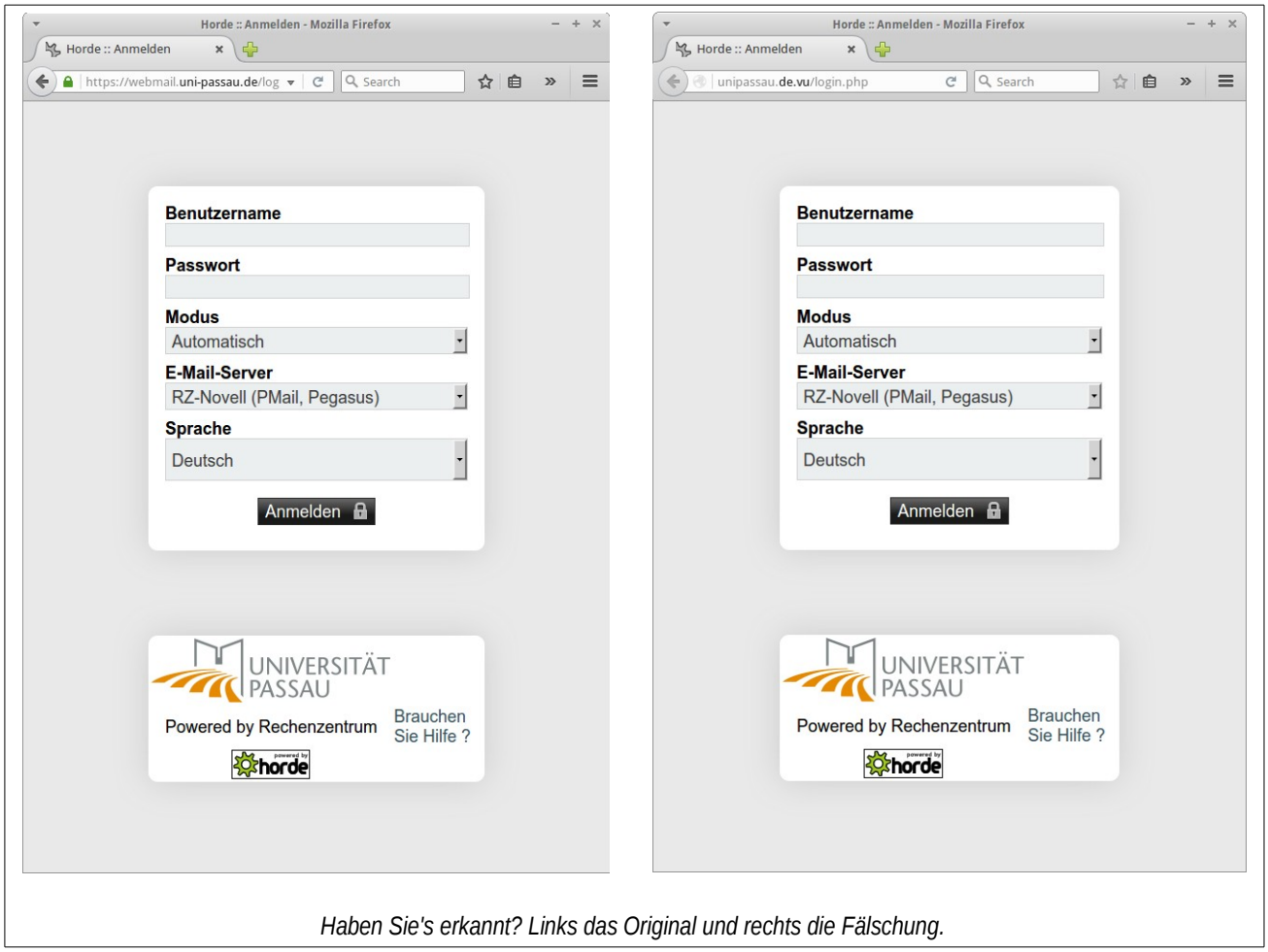
¶ Das Rechenzentrum und das InteLeC-Zentrum gehen zum 01.01.2016 im neuen "Zentrum für Informationstechnologie und Medienmanagement" (ZIM) auf. Daher wird in diesem Schreiben bereits die Bezeichnung "ZIM" verwendet.

Absender beliebig fälschen können. Eine E-Mail ist per se zunächst ebenso vertrauenswürdig einzustufen wie etwa eine Postkarte, die mit der normalen Postzustellung ankommt.

Ob eine E-Mail tatsächlich authentisch ist, kann im Einzelfall nur von Ihnen selbst durch Bewertung des Inhalts im Kontext des (vermeintlichen) Absenders festgestellt werden. Im Zweifelsfall empfiehlt es sich, beim vermuteten Absender **rückzufragen**.

Der Support des ZIM wird Sie **niemals** per E-Mail dazu auffordern, Ihre Zugangsdaten per E-Mail zu versenden bzw. auf Webseiten "zwecks Überprüfung" o. ä. einzugeben.*

Bitte löschen Sie Mails mit derartigem Inhalt. Antworten Sie nicht darauf und klicken Sie auch ggf. in den E-Mails enthaltene Links nicht an. Falls Sie trotz dieser Empfehlung Links anklicken, werden Sie möglicherweise auf Webseiten geleitet, die unter Umständen den Originalwebseiten der Universität täuschend ähnlich sehen.



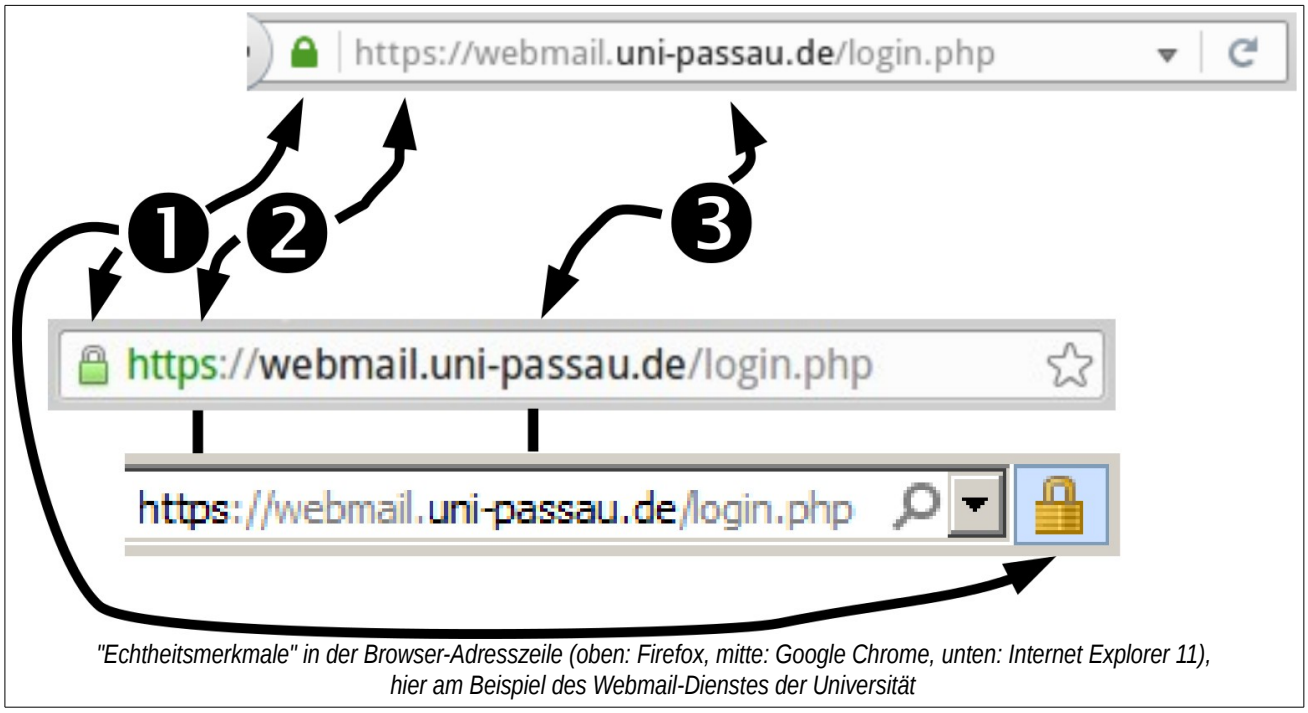
Haben Sie's erkannt? Links das Original und rechts die Fälschung.

In Zweifelsfällen wenden Sie sich bitte an den Support des ZIM (Haus-Tel. 1888, E-Mail support@zim.uni-passau.de).

* Die einzige E-Mail, die Sie vom Rechenzentrum (künftig: ZIM) im Zusammenhang mit Ihrer Benutzerkennung erhalten, ist die "Erinnerungsmail" an die notwendige Änderung Ihres Passwortes. Diese Mail enthält bereits Ihre persönliche Anrede und Ihre Kennung sowie einen Hinweis auf die Webseite des Rechenzentrums, auf der das Passwort geändert werden kann, aber keinen direkten Link zu einer Passwort-Änderungsseite.

Wir empfehlen, die Adressen von Webseiten, auf denen Sie bekannterweise Zugangsdaten eingeben müssen (z. B. Webmail, Passwortänderungen, Stud.IP, HISQIS) in Ihrem Browser als **Favoriten** (Bookmarks) zu speichern und die betreffenden **Seiten ausschließlich über diesen Weg** aufzurufen. Alternativ kann die Einstiegsseite (z. B. www.uni-passau.de) aufgerufen und dann durch Navigation auf der Webseite das jeweilige Ziel angesteuert werden.

Wie können Sie im Zweifelsfall erkennen, ob Sie wirklich auf einer authentischen Webseite der Universität gelandet sind, auf der Sie ohne Bedenken Ihre Zugangsdaten eingeben können?



"Echtheitsmerkmale" in der Browser-Adresszeile (oben: Firefox, mitte: Google Chrome, unten: Internet Explorer 11), hier am Beispiel des Webmail-Dienstes der Universität

Die folgenden drei Merkmale müssen vorhanden sein, ansonsten sollten Sie davon ausgehen, dass Sie auf einer "Phishing-Webseite" gelandet sind:

❶ Die "Echtheit" der Webseite ist vom Browser geprüft (in den aktuellen Versionen von Firefox und Chrome mit einem grünen Schloss gekennzeichnet, im aktuellen Internet Explorer mit einem Schloss auf blauem Hintergrund).

❷ Die Adresse der Webseite beginnt mit "https".

❸ Der Domainname endet auf "**.uni-passau.de**". (Achtung: Ähnlich klingende oder geschriebene Domainnamen, wie etwa uni-pasau.de, uni-passau.co, unipassau.de.vu, haben mit der Universität Passau nichts zu tun und sind ein deutliches Zeichen für betrügerische Absichten!)

Benutzerkennungen, die per Phishing-Angriff ergaunert wurden, werden meist für illegale Aktionen missbraucht, z. B. zum Versenden von Spam-Mail oder auch für strafrechtlich relevante Aktivitäten im Internet unter der "geklauten" Identität. Dies

kann schlimmstenfalls zu zivil- und strafrechtlichen Konsequenzen für die Universität und Sie als Inhaber der Benutzerkennung führen.

Bitte beachten Sie die folgenden **Regeln** zum Umgang mit Ihrem Benutzerpasswort:

- Geben Sie Ihr Passwort **niemals auf "fremden" Webseiten** ein (siehe Hinweise oben).
- Gebrauchen Sie Ihr Passwort **ausschließlich in vertrauenswürdigen IT-Umgebungen**, also insbesondere nicht auf fremden Rechnern (z. B. in Internet-Cafés).
- Ihr Passwort ist Ihr eigenes, persönliches Geheimnis. Geben Sie es daher **niemals an Dritte** weiter.
- Verwenden Sie Ihr Uni-Passwort **nicht bei anderen Diensten** (z. B. Ihrem privaten Webmail-Account, Ihrem Amazon-Konto, ...).

Für weitere Fragen stehe ich in meiner Eigenschaft als IT-Sicherheitsbeauftragter der Universität Passau gerne zur Verfügung.

Freundlichen Gruß,

Dr. Christian Rank