

Universität Passau · Rechenzentrum · D-94030 Passau

An die Angehörigen
der Universität Passau

Telefon	0851 509-1838 0851 509-1801 (Sekretariat)
Telefax	0851 509-1802
e-mail	christian.rank@uni-passau.de
Zeichen	20170622_phishing
Datum	26.06.2017

Grundlegende Prinzipien zum Umgang mit E-Mails und Passwörtern

Sehr geehrte Damen, sehr geehrte Herren,

eine kürzlich erfolgte Phishing-Attacke auf Angehörige der Universität Passau, bei der auf einer vorgeblichen (!) Webseite der Universität die Daten der ZIM-Kennung abgefragt wurden, möchte ich zum Anlass nehmen, auf die grundlegenden **Prinzipien im Umgang mit E-Mails** hinweisen:

1. Der **Absender** einer E-Mail kann **beliebig gefälscht** werden. Lassen Sie sich nicht dazu verleiten, eine E-Mail für authentisch zu halten, nur weil Sie den (vermeintlichen) Absender kennen. Wenn Sie sich nicht sicher sind, fragen Sie beim Absender nach. Sind angeblich Sie selbst der Absender, ist ebenfalls besondere Vorsicht angebracht. **Bitte öffnen Sie im Zweifelsfall weder Anhänge noch klicken Sie auf Links!**
2. **Links** in E-Mails können auf Webseiten führen, die **Schadcode** enthalten. Ebenso kann das Ziel eines Links eine sog. **Phishing-Webseite** sein, auf der Sie zur Preisgabe vertraulicher Daten (z. B. Ihrer Passwörter) verleitet werden sollen. Darüber hinaus kann das Ziel eines Links verdeckt sein, so dass Sie dem Link nicht ansehen können, zu welcher Webseite er schließlich führt. **Sie sollten keinesfalls auf Links klicken, die Sie unerwartet erhalten!**
3. **Anhänge** (sog. Attachments) können **Schadcode** enthalten. Sie sollten Anhänge nur dann öffnen, wenn alle der folgenden Bedingungen erfüllt sind:
 - Die E-Mail stammt **wirklich** von einem Ihnen **bekanntem Absender** und Sie **erwarten** von diesem Absender einen entsprechenden Anhang,
 - Die Mail und der Anhang entspricht in Form und Struktur den bisherigen **Kommunikationsgewohnheiten** mit Ihrem E-Mail-Partner (verdächtig ist

z. B. wenn Sie eine E-Mail auf Englisch erhalten, wenn Sie bisher auf Deutsch kommuniziert haben),

- Der Anhang (oder der Inhalt eines Dateiarchivs im Anhang) enthält **keine** Dateien mit **kritischen Dateitypen** (u. a. BAT, COM, JS, EXE, PIF, SCR, VBS).

Bitte beachten Sie, dass auch **Office-Dokumente** durch darin **enthaltene Makros gefährlich sein können**. In der Standardkonfiguration von Microsoft Office werden Sie beim Öffnen eines Dokuments gewarnt, wenn es Makros enthält:



Die angebotene Möglichkeit, die Makros (in der Warnung von Microsoft fälschlicherweise als "Inhalt" bezeichnet) zu aktivieren, sollten Sie zunächst nicht wahrnehmen! Erst wenn Sie nach genauer Prüfung des Dokumentinhalts und ggf. Rücksprache mit dem Absender die Notwendigkeit sehen, Makros in dem entsprechenden Dokument zu aktivieren, können Sie durch Betätigen der entsprechenden Schaltfläche in Office die Ausführung von Makros in dem betreffenden Dokument zulassen.

4. Im übrigen verweise ich auf die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum **"gesunden Menschenverstand"**.¹

Weitere Informationen zur Phishing-Thematik finden Sie beispielsweise auf den Webseiten des "BSI für Bürger".² Ebenso zum Thema Schadcode.³

Bitte nehmen Sie Kontakt mit dem ZIM-Support auf,⁴ wenn Sie vermuten, Opfer einer Phishing-Attacke geworden zu sein. Wenn sich ein Fremder in Besitz Ihres Passworts gebracht hat, kann er nicht nur auf Ihre Dateien zugreifen, sondern u. a. auch Mails in Ihrem Namen verschicken! **Behandeln Sie daher Ihr Passwort stets vertraulich**. Tippen Sie Passwörter grundsätzlich nur auf vertrauenswürdigen Geräten ein. Auf Webseiten, die nicht zur Uni Passau gehören, dürfen Sie Ihr ZIM-Passwort keinesfalls eingeben.

Wenn Sie einen Befall Ihres Systems mit Ransomware oder auch jeglicher anderer Schadsoftware vermuten, unterbrechen Sie bitte unverzüglich die Verbindung des Gerätes zum Datennetz und wenden Sie sich an den Support des ZIM.

gez. Dr. Christian Rank, CISO Uni Passau

1 https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Menschenverstand/menschenverstand_node.html

2 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html

3 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Schadprogramme/schadprogramme_node.html

4 <http://www.zim.uni-passau.de/kontakt/>