UNIVERSITÄT BAYREUTH

IT-SERVICEZENTRUM
Wir kümmern uns.

Redaktion: Ariadne Engelbrecht
Stand: Juni 2015

News 15/03

Sicherheitsfaktor Mensch

Kennen Sie das? Sie bekommen eine scheinbar vertraute E-Mail. Auch die Frage nach Ihrem Passwort schreckt nicht ab - immerhin ist der Absender bekannt - doch plötzlich merken Sie, dass die eigenen Anmeldedaten nicht mehr stimmen. Was ist da los? Sind Sie vielleicht Opfer einer Phishing-Mail geworden?

Phishing-Angriffe erkennen und abwehren

Das Wort Phishing setzt sich aus „Password" und „fishing" zusammen, zu Deutsch „nach Passwörtern angeln". Immer öfter fälschen Phishing-Betrüger E-Mails und Internetseiten und haben damit leider einen allzu oft erfolgreichen Weg gefunden, um an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern zu kommen. Vor einigen Wochen haben Phishing-Mail-Betrüger eine gefälschte Uni-Mailserver-Anmeldeseite nachgebaut, um die Zugangsdaten von Uniangehörigen gezielt „abzufischen" und diese später zu missbrauchen.

Hier gefahrlos zu sehen: ► http://www.rz.uni-bayreuth.de/de/Aktuelles/SI-News/Phishing_mail/index.html ◄

Haben Sie diesen Betrugsversuch gleich erkannt? Und ***woran genau*** können Sie solche Phishing-Angriffe erkennen? ►► Informieren Sie sich auf den ITS-Webseiten unter der Rubrik „IT-Sicherheit" über „Phishing-Angriffe".

Interessant: Sie können Ihr Passwort problemlos bei uns im ITS-Portal* ändern!

„In 7 Schritten einfach sicher*er* sein"

In der Rubrik „IT-Sicherheit" auf der ITS-Website finden Sie den zum Download bereitgestellten Sicherheits-Flyer in deutscher und englischer Sprache. Er enthält einfach umzusetzende und wirksame Tipps, wie Sie sich selbst und Ihre Daten in Privat- und Berufsleben mit gezielten Maßnahmen besser schützen können! IT-Sicherheit unterscheidet nicht zwischen Privat- und Arbeitsrechner. Sicherheit geht eben alle, immer, überall etwas an!

Falls Sie diese Regeln schon alle kennen und beherzigen - nun vielleicht freut sich Ihr Kollege oder ein Mensch aus Ihrem Privatleben über diesen Flyer? Daher dürfen Sie den Link zum Flyer und auch die gedruckte Form von uns aus gerne weitergeben.

Interessant: Der Flyer kann in gedruckter Form (deutsch und englisch) per Mail bei Ariadne.Engelbrecht@uni-bayreuth.de angefordert und am Lehrstuhl verteilt werden!

---

* **Wie öffne ich das ITS-Portal?**

Gehen Sie auf der Homepage der Universität auf „Universität" > „Service" > „Service für Beschäftigte" > „Onlinedienste" > „Für alle Mitarbeiter". Dort finden Sie neben dem Telefonbuch, der Raumverwaltung und u.a. auch einen Link auf das ITS-Portal.

———— Alternativ der direkte Link: https://portal.rz.uni-bayreuth.de.

Bitte machen Sie uns nicht nur auf Rechtschreibfehler, sondern gerne auch auf andere Korrekturvorschläge, Ihre Wünsche und Anregungen aufmerksam!

Sophos Server zieht um!

Der bestehende Sophos Updateserver im ITS wird bald durch einen neuen Server ersetzt. Alle Beschäftigten müssen daher bis spätestens zum 30.11.2015 die unten erklärten Änderungen an der Konfiguration von Sophos Antivirus durchführen - aber keine Angst, soviel ist das gar nicht.

SOPHOS
Security made simple.

Was muss ich tun?

Prinzipiell gilt die gedankliche Trennung in…

… Computer, die nur *intern auf dem Campus* verwendet werden und eine IP-Adresse im Bereich 132.180.X.X haben:

▸ Diese müssen keine Änderungen durchführen!

Sie verwenden weiterhin für den AutoUpdate Dienst die URL:

Windows: http://sav9upd.uni-bayreuth.de/SAVSCFXP/

Mac OS X: http://sav9upd.uni-bayreuth.de/ESCOSX/

… alle Computer, die *außerhalb des Campusnetzes* verwendet werden:

▸ Diese müssen künftig für den AutoUpdate Dienst von Sophos folgende URL eintragen:

Windows: http://sav9updext.uni-bayreuth.de/SAVSCFXP/

Mac OS X: http://sav9updext.uni-bayreuth.de/ESCOSX/

Um diese Änderungen durchzuführen oder einfach um nachzuschauen, was bei Ihnen eingetragen ist, starten Sie bitte das Programm *Sophos Endpoint Security and Control*.

Danach im Menü *Konfigurieren* den Punkt *Updates* auswählen und die entsprechenden Zugangsdaten (vgl. oben) eintragen.

Für alle gilt:

Als Authentifizierung wird Ihre BT-Kennung und das dazu gehörige Passwort verwendet.

Und mehr?? Ist es nicht.