Brauche ich ein Passwort?

Um einen Benutzer an einem Computersystem oder einer Datenbank eindeutig identifizieren zu können, benötigt dieser meist eine Zugangskontrolle in Form von Benutzername und dem dazugehörigen Passwort.

Hohes Risiko – Missbrauch vermeiden

- Ihre Passwörter an Dritte weitergeben
- Passwörter in digitaler Form auf dem Computer abspeichern
- leicht zu erratende Passwörter verwenden. z.B. Namen, Orte, Geburtstage, etc.
- das gleiche Passwort über einen längeren Zeitraum beibehalten

Die Mehrfachnutzung von Passwörtern und insbesondere in der Kombination von Benutzername und Passwort stellt ein erhebliches Sicherheitsrisiko dar.

Passwortklau und Phishing

Die Universität Bayreuth (z. B. Verwaltung, Studentenwerk, IT-Servicezentrum, etc.) sowie alle vertrauenswürdigen Institutionen (z. B. Banken, etc.) fragen Sie niemals über E-Mail, mündlich oder auch fernmündlich nach Ihren TANs und Passwörtern!

Was sind sichere Passwörter?

Ein sicheres Passwort sollte eine Mindestlänge von acht Zeichen und aus einer alphanumerischen Kombination, ohne offensichtlichen Sinnzusammenhang unter Einbindung von Gross-/Kleinbuchstaben (ohne Sonderzeichen wie z. B. !"§$%&/ß und Umlaute wie z. B. äüö), zusammengesetzt sein:

uwe **MHBi4DHa2T**

unsicher — sicher

Verknüpfen Sie Ihr Passwort mit persönlichen Erlebnissen oder Erinnerungen.

Lassen Sie Ihren Ideen freien Lauf, seien Sie kreativ!

Beispiele

Der **B**all **i**st **r**und **u**nd **m**uss **i**ns **E**ckige — **DBirumiE**

Mein **H**und **B**ello **i**sst **4** **D**osen **H**undefutter **a**n **2** **T**agen — **MHBi4DHa2T**

Haustür **2** **E**tage **l**inke **T**ür **3** **Z**immer **r**echte **T**ür — **H2ElT3ZrT**

So werden es Passwortdiebe wesentlich schwerer haben, Ihr Passwort zu erraten oder durch Software zurück zu berechnen!

HTTPS- Verschlüsselung

Achten Sie beim Online-Banking oder dem Versenden von vertraulichen Informationen bzw. persönlichen Daten (z. B. Bestellungen) auf eine verschlüsselte Verbindung.
Diese erkennt man am https:// anstatt http:// und an einem geschlossenen Schlosssymbol.

Flyer online: Deutsch Englisch

Sicherheit & Computerschutz

... Beschäftigte ... Studierende

Wie kann ich mich schützen?

In 7 Schritten...

Firewall aktivieren

1 Alle modernen Betriebssysteme haben eine integrierte Firewall, die den eingehenden Netzwerkverkehr untersucht und Angriffe automatisch abblockt. Aus sicherheitstechnischer Sicht sind diese integrierten Firewalls absolut ausreichend. Sofern diese aktiviert sind ist der Einsatz einer zusätzlichen „Personal Firewall" also nicht notwendig.

Virenscanner verwenden

2 Unter Microsoft Windows Betriebssystemen ist die Verwendung eines Virenscanners unabdingbar. Da jeden Tag neue Schadsoftware verbreitet wird, ist es zudem besonders wichtig den eingesetzten Virenscanner regelmäßig mit neuen Signaturupdates zu versorgen, um sich auch gegen die neuesten Bedrohungen zu schützen – dies geschieht bei der richtigen Konfiguration meist automatisch, sobald das Gerät mit dem Internet verbunden ist.
Die Universität Bayreuth stellt die Software „Sophos AntiVirus" kostenlos zum Download zur Verfügung. Für den Privatgebrauch gibt es auch diverse kostenlose Virenscanner wie z.B. Microsoft Security Essentials, der ab Windows 8 unter dem Namen „Windows Defender" bereits im Betriebssystem integriert ist und nur aktiviert werden muss.

Wachsames Surfverhalten

3 Die meisten Computerschädlinge gelangen durch infizierte Webseiten auf den Computer – das können illegale Download-/Streaming-Portale sein, aber auch ungepflegte „reguläre" Seiten. Bereits der Aufruf einer derartigen Webseite genügt für eine Infektion über sogenannte Drive-by-Downloads – Sie als Nutzer bekommen davon absolut nichts mit. Meiden Sie daher grundsätzlich Webseiten mit derartigen Inhalten, sowie auch vermeintliche Gewinnversprechungen oder Meldungen à la „Ihr Computer ist zu langsam/infiziert, bitte Klicken Sie hier". Seien Sie vorsichtig und klicken Sie lieber einmal zu wenig als einmal zuviel!

If it sounds too good to be true...

Weitere Informationen: www.bsi.bund.de

System aktuell halten

4 Sicherheitslücken sind Fehler im Betriebssystem bzw. in darauf installierter Software und werden von Schadprogrammen genutzt, um Ihren Rechner zu infizieren.
Die Software-Hersteller veröffentlichen in regelmäßigen Abständen wichtige Updates, um diese Lücken zu stopfen – diese sollten Sie immer sofort einspielen. Jedes moderne Betriebssystem hat eine Updateverwaltung für Sicherheitsupdates eingebaut. Hier empfiehlt es sich, die automatische Updateinstallation zu aktivieren.
Installierte Programme muss man einzeln aktuell halten. Viele Programme prüfen automatisch auf neue Updates, bei manchen muss man allerdings manuell auf Updates prüfen und diese einspielen.

Regelmäßige Datensicherung

5 Ein aktuelles Backup schützt Ihre Daten nicht nur im Falle einer Schadsoftware-Infektion, sondern auch bei plötzlichen Hardwareausfällen müssen Sie so nicht auf Ihre wertvollen Daten verzichten.
Erstellen Sie das Backup z.B. auf eine externe Festplatte oder ein NAS (=Network Attached Storage), das am besten räumlich getrennt von Ihrem Rechner steht, damit Sie auch nach einem Brand oder Wasserschaden noch Zugriff auf Ihre Daten zu haben.

Betrugsversuche erkennen

6 Sowohl beim Surfen im Internet, als auch im eigenen E-Mail-Konto wird man häufig Opfer von Betrugsversuchen. Die meisten dieser E-Mails sind an der schlechten Sprache leicht zu erkennen, einige sind aber inzwischen so gut gefälscht, dass selbst Profis diese erst bei sehr genauem Hinsehen als solche identifizieren können.
Die Verwendung Ihres Vor- und Nachnamens ist kein sicheres Erkennungszeichen für einen seriösen Absender mehr – besonders nicht, wenn Ihre Mail-Adresse Ihren Vor- und Nachnamen beinhaltet. Überprüfen Sie immer genau den „richtigen" Absender, klicken Sie im Zweifelsfall niemals auf enthaltene Links und öffnen Sie keinesfalls Anhänge!

Verhalten bei Infektionsverdacht

7 Sollten Sie die Befürchtung haben, dass Ihr Rechner mit Schadsoftware infiziert wurde, trennen Sie umgehend die Verbindung zum Internet, fahren Sie den Rechner ordnungsgemäß herunter und wenden Sie sich sofort an das IT-Servicezentrum. Wir helfen Ihnen gerne und so haben Sie die besten Chancen auf eine erfolgreiche Desinfektion.

...einfach *sicherer* sein.