SICHERHEITSREGELN ZUM SCHUTZ VON PC UND DATEN

1. *Software auf dem aktuellen Stand halten*

Betriebssysteme und Anwendungen weisen immer wieder Schwachstellen auf, die die Sicherheit Ihres Computers gefährden. Installieren Sie regelmäßig die "Sicherheits-Updates", "Patches" und "Service Packs" der Hersteller, um Schwachstellen zu beseitigen.

Sicher ist: Besser rechtzeitig die Software aktualisieren als alles neu installieren zu müssen!

2. *Aktuellen Virenscanner verwenden*

Ein aktueller Virenscanner gehört zum Basisschutz eines jeden Computers. Achten Sie darauf, dass dieser aktiviert ist und auf dem aktuellen Stand gehalten wird.

Sicher ist: Virenschutz ist Basisschutz, kein Luxus!

3. *Daten mit einer Firewall schützen*

Eine Firewall schützt Ihren Computer vor unberechtigten Zugriffen aus dem Internet bzw. aus einem Netzwerk, in dem Sie arbeiten.
Wenn Sie mit Ihrem Computer im Internet oder einem Netzwerk arbeiten, stellen Sie sicher, dass eine lokale Software-Firewall installiert und aktiviert ist. Aktuelle Betriebssysteme (Windows, Linux, Mac OS X) bieten Ihnen bereits eine integrierte Firewall für einen Basisschutz an.

Sicher ist: Niemals ohne Firewall ins Netz!

4. *Sichere Passworte verwenden und sicher speichern*

Einfache und kurze Passworte sind leicht zu merken. Aber sie sind nicht sicher.
Für eine ausreichende Passwortsicherheit beachten Sie bitte die folgenden Punkte:

- Nutzen Sie mindestens acht Zeichen mit Ziffern, Buchstaben und/oder Sonderzeichen.
- Verwenden Sie keine Trivialpassworte wie Namen, Geburtstage oder Wörter, die in Wörterbüchern stehen.
- Benutzen Sie unterschiedliche Passworte für unterschiedliche Bereiche (Universität, Internet-Shopping, soziale Netzwerke etc.).
- Behandeln Sie Ihr Passwort wie die PIN Ihrer Bankkarte. Geben Sie es nicht weiter, auch nicht wenn Sie dazu aufgefordert werden. Das IT-Personal der Universität wird Sie nie um die Herausgabe Ihres Passwortes bitten.
- Notieren Sie Passworte niemals sichtbar, wechseln Sie es regelmäßig und speichern Sie es wenn überhaupt nur geschützt auf Ihrem Computer ab. Nutzen Sie dazu am besten bewährte Passwort-Tresore:

Sicher ist: Nutzen Sie Passwort-Phrasen, um sich sichere Passwörter einfach zu merken.
Beispiel: In der Mensa gibt es freitags immer Fisch! Die Anfangsbuchstaben des Satzes ergeben das Passwort *1dMgefiF!*. In diesem Fall wird das Wort "in" durch eine Zahl ersetzt.

5. *Nicht mit Administratorrechten arbeiten*

Wenn Sie mit Administratorrechten auf ihrem Computer arbeiten, haben auch Schadprogramme uneingeschränkten Zugriff auf Ihr System und können erst so Ihre volle Wirkung zu entfalten.

Arbeiten Sie im Alltag mit einem Benutzer-Konto mit eingeschränkten Rechten. Administratorrechte sind nur notwendig, um z.B. Änderungen an der Konfiguration vorzunehmen.

Sicher ist: Eingeschränkte Rechte schützen Ihren Computer im Alltag!

6. *Vorsicht bei unbekannten E-Mail-Anhänge*

Eine große Anzahl von "Malware" (schädliche Software wie Viren, Würmer oder Trojaner) verbreitet sich per E-Mail. Öffnen Sie nicht leichtfertig E-Mail-Anhänge von Absendern, die Sie nicht kennen bzw. von welchen Sie keinen Anhang erwarten.
Jeder Anhang den Sie öffnen, egal, wie vertrauenswürdig er erscheint, kann die Sicherheit Ihres Computers gefährden.

Sicher ist: E-Mail-Anhänge besser einmal zu wenig als einmal zu viel öffnen!

7. *Daten regelmäßig sichern*

Eine regelmäßige Sicherung ("Backup") Ihrer wichtigen Daten schützt diese vor Verlust. Die meisten Betriebssysteme (Windows, Linux, Mac OS X) bieten Ihnen bereits integrierte Funktionen für eine einfache Datensicherung an.

Sicher ist: Sichern Sie Ihre Daten rechtzeitig und regelmäßig gegen Verlust (Save early, save often)!

8. *Sensible Daten durch Verschlüsselung schützen*

Sichern Sie Ihre vertraulichen Daten gegen einen unberechtigten Zugriff durch Dritte indem Sie diese verschlüsseln. Aktuelle Betriebssysteme (Windows, Linux, Mac OS X) bieten Ihnen dazu bereits integrierte Mechanismen an. Alternativ kann auch kostenlose und quelloffene Software wie beispielsweise Truecrypt genutzt werden.
Vergessen Sie im Gegenzug nicht Passwörter für verschlüsselte Daten sicher zu hinterlegen. Gehen diese verloren, sind die Daten für Sie unbenutzbar.

Sicher ist: Mit Verschlüsselung schützen Sie vertrauliche Daten vor Dritten!

9. *Sensible Informationen nicht leichtfertig preisgeben*

Werden Sie hellhörig, wenn Sie mit einem (augenscheinlich) plausiblen Grund um die Herausgabe von vertraulichen Informationen wie z. B. Ihrem Passwort gebeten werden. Die Beschäftigten der Universität werden Sie nie um die Herausgabe nach vergleichbaren Informationen bitten.
Prüfen Sie bei solchen Fragen im Zweifelsfall die Identität der Anrufer indem Sie diese unter der Durchwahl aus dem offiziellen Telefonverzeichnis zurückrufen.

Sicher ist: Sensible oder persönliche Informationen niemals an unbekannte Personen herausgeben!

10. *Aufmerksam, kritisch und informiert bleiben*

Sicherheit ist kein Produkt, das man kaufen, installieren und vergessen kann. Ein aktuelles System mit Virenscanner und Firewall bietet nur einen technischen Basisschutz.
Bleiben Sie aufmerksam, kritisch und informiert, wenn es um die Sicherheit Ihres Computers geht. Gedankenlosigkeit oder Vertrauensseligkeit hebeln jeden technischen Schutz aus. Egal ob jemand bösartige Software auf Ihrem Computer installieren will oder es auf das Geld auf Ihrem Konto abgesehen hat. Er wird mit allen Tricks versuchen, sein Ziel zu erreichen.

Sicher ist: Das Gehirn zusammen mit dem Computer einzuschalten!

Quelle: https://www.uni-bielefeld.de/it-sicherheit/Studierende/goldene_regeln_st.html