SICHERHEITSHINWEISE

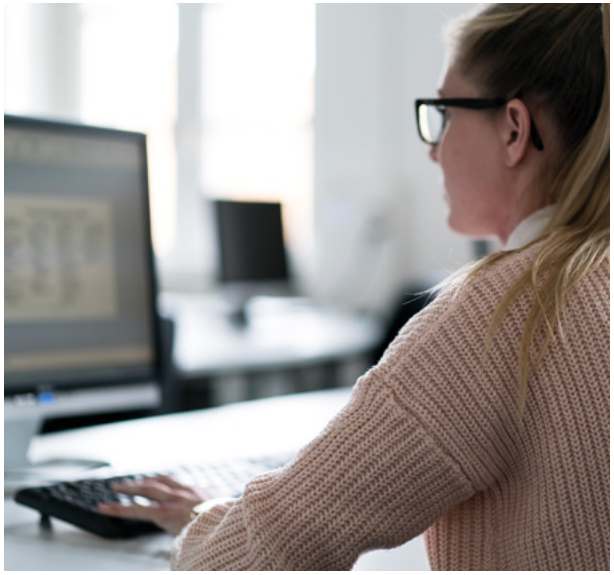
Mit der Entwicklung der Informationstechnik werden immer mehr Informationen verarbeitet und gespeichert.

Damit ist auch die Verantwortung des Einzelnen mit dem Umgang der Informationstechnik gestiegen. Die Sicherheit in der Informationstechnologie umfasst die Einhaltung bestimmter Sicherheitsstandards, um die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen zu gewährleisten.

Die hier aufgelisteten Sicherheitsanregungen geben dem einzelnen Anwender einige Hinweise für einen sicheren Umgang mit seinem PC.

UMGANG MIT PASSWÖRTERN UND ZUGANGSDATEN

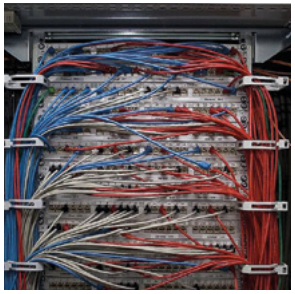
- Passwörter sind mindestens acht Zeichen lang und bestehen aus einer Kombination von Zahlen und Buchstaben.
- Halten Sie Ihre Passwörter geheim und geben Sie diese nicht an Dritte weiter.
- Wechseln Sie Ihre Passwörter halbjährlich.
- Benachrichtigen Sie das Dezernat Studentische Angelegenheiten, sobald jemand vom Passwort Kenntnis erlangt hat.
- Speichern Sie keine Passwörter und andere Zugangsdaten auf Ihrem Computer.
- Geben Sie Ihr Hochschul-Passwort niemals auf Webseiten ein, die nicht zur Hochschule (www.hs-harz.de) gehören.



MASSNAHMEN ZUM SCHUTZ IHRES RECHNERS

Viren, Würmer und Trojaner sind Programme, die Daten vernichten, verändern oder löschen können. Sie können sich selbstständig verbreiten und reproduzieren. Und sie können vertrauliche Informationen, die auf Ihrem Rechner — ob PC oder Smartphone — gespeichert sind, ausspionieren.

- Mögliche Sicherheitseinstellungen Ihres Geräts sollten eingeschaltet sein.
- Nutzen Sie Sperrcodes und Passwörter.
- Achten Sie darauf, dass Ihr Betriebssystem und der Browser auf dem aktuellen Stand sind.
- Setzen Sie einen Virenscanner mit einer täglichen Aktualisierung auf Ihrem Computer ein.
- Setzen Sie eine Anti-Spysoftware auf dem PC ein.
- Aktivieren Sie den Makro-Virenschutz der Anwendungsprogramme und beachten Sie die Warnmeldungen.
- Wählen Sie die höchste Stufe der Sicherheitseinstellungen bei Internet-Browsern aus.
- Vorsicht bei der Aktivierung der aktiven Inhalte (ActiveX, Java, VBScript), denn in diesen können Dialer oder andere Programme installiert sein.
- Prüfen Sie eingehende Daten von CD ROMs, USB Sticks mit einem Virensuchprogramm.
- Setzen Sie eine Firewall ein.
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen und prüfen Sie die Zugriffsberechtigungen.
- Deinstallieren Sie nicht benötigte Programme.



SICHERUNG DER DATEN AM ARBEITSPLATZ-PC

- Die Durchführung von Wartungs- und Reparaturarbeiten sollte ausschließlich durch den Administrator erfolgen.
- Nehmen Sie keine Änderungen der bestehenden Konfiguration vor.
- Melden Sie Unregelmäßigkeiten dem zuständigen Administrator.
- Speichern Sie regelmäßig Ihre Daten auf den vom Rechenzentrum angebotenen Backup-Systemen (Archiv, Filer) oder externen Datenträgern. Achten Sie darauf, externe Datenträger eindeutig und aktuell zu beschriften.

SCHUTZ DER DATEN VOR UNBERECHTIGTEM ZUGRIFF UND MANIPULATION AM ARBEITSPLATZ-PC

- Lassen Sie Ihren Arbeitsplatz nicht unbeaufsichtigt.
- Benutzen Sie einen Bildschirmschoner mit Passwort.
- Schließen Sie alle Anwendungen und melden Sie sich ab bzw. schalten Sie Ihren PC beim Verlassen des Arbeitsplatzes aus.

SICHERER UMGANG MIT E-MAILS

Schadprogramme werden häufig mit E-Mails versendet, hier einige Tipps, wie Sie sich schützen können:

- Tragen Sie Ihre E-Mailadresse im Web nicht überall ein, hüten Sie diese eher wie ein Geheimnis.
- Richten Sie sich für bestimmte Aktivitäten im Netz eine zweite E-Mail-Adresse ein.
- Sinnlose E-Mails unbekannter Absender sollten Sie ungeöffnet löschen.
- Öffnen Sie keine SPAM E-Mails, Spammer nutzen oft HTML-Formatierte Mails, um die Gültigkeit der E-Mail-Adresse zu prüfen.
- Öffnen Sie Anhänge nur von erwarteten E-Mails.
- Lassen Sie Vorsicht walten bei Anhängen mit ausführbaren Dateien (*.exe, *.com, *.scr).
- Seien Sie ebenfalls vorsichtig bei mehreren E-Mails mit gleich lautendem Betreff.
- Prüfen Sie E-Mails von bekannten Absendern, ob der Text der Nachricht zum Absender passt.
- Vermeiden Sie das Versenden von unnötigen E-Mails mit Scherzprogrammen etc., da diese eventuell einen Computer-Virus enthalten.
- Prüfen Sie gelegentlich, ob E-Mails im Ausgangspostkorb stehen, die Sie nicht selbst verfasst haben.
- Verbieten Sie den automatischen Versand.
- Nutzen Sie digitale Signaturen und Verschlüsselungsverfahren für die Übertragung von Informationen per E-Mail.
- Verwenden Sie ein aktuelles Virenschutzprogramm.
- Öffnen Sie keine unbekannten Links in E-Mails und geben Sie keine Passwörter ein. Benachrichtigen Sie den Helpdesk, wenn Sie Ihr Passwort eingegeben haben und vermuten, dass es sich um ein Schadprogramm handelt.

SICHER UNTERWEGS IM INTERNET

Ob per Browser oder Smartphone

- Nutzen Sie Verschlüsselungsverfahren für die Übertragung von sensiblen Informationen über das Internet (z.B. Zugangsdaten, wie Passworte und Nutzerkennungen), gekennzeichnet sind diese Verbindungen durch https:// in der Webadresse und einem Schloss in der Statuszeile.
- Das hinterlegte Zertifikat muss von einer anerkannten Stelle ausgestellt sein.
- Laden Sie Programme nur von vertrauenswürdigen Seiten (Originalseiten des Erstellers) herunter.
- Führen Sie einen Viren-Check der heruntergeladenen Dateien mit einem aktuellen Virenschutzprogramm durch.
- Prüfen Sie die Größe bzw. die Prüfsumme des Downloads, Abweichungen können aus unzulässigen Veränderungen resultieren.

KONTAKT

www.hs-harz.de
Hochschule Harz, Friedrichstraße 57-59, 38855 Wernigerode

Helpdesk Rechenzentrum
E-Mail: helpdesk@hs-harz.de

IT-Sicherheitsbeauftragte des Rechenzentrums
Sandra Thielert
Tel.: +49 3943–659-907
E-Mail: sthielert@hs-harz.de

2103

▲ Hochschule Harz

Hochschule für angewandte Wissenschaften

Rechenzentrum

Sicherheitshinweise zum Arbeiten mit dem Computer