HOCHSCHULE harz
Hochschule für angewandte Wissenschaften (FH)
Wernigerode Halberstadt

Sicherer Umgang mit E-Mails

Schadprogramme werden häufig in E–Mailanhängen versendet, daher sind hier einige Regelungen im Umgang mit E–Mails aufgelistet.

- Tragen Sie Ihre E–Mailadresse im Web nicht überall ein, hüten Sie diese eher wie ein Geheimnis
- Richten Sie sich für Webaktivitäten 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 vertrauenswürdigen E–Mail–Adressen
- 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 u. a., da diese eventuell einen Computer–Virus enthalten
- Prüfen Sie gelegentlich, ob E–Mails im Ausgangs–postkorb stehen, die Sie nicht selbst verfasst haben
- Verbieten Sie den automatischen Versand
- Nutzen Sie digitale Signaturen und Verschlüsselungs verfahren für die Übertragung von Informationen per E–Mail

Sicherheit bei Downloads im Internet

Jegliche Daten, Dateien und Programme, die aus dem Internet abgerufen werden, stellen einen Hauptverbrei–tungsweg für Viren und Trojaner dar.

- 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
- Nutzen Sie Verschlüsselungsverfahren für die Über–tragung von sensiblen Informationen über das Internet (z. B. Zugangsdaten, wie Passworte und Nutzerken–nungen), gekennzeichnet sind diese Verbindungen durch https:// in der Webadresse und einem Schloss in der Statuszeile
- Laden Sie Programme nur von vertrauenswürdigen Seiten (Originalseiten des Erstellers) herunter

Rechenzentrum

Sicherheitshinweise für PC-Nutzer

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 Endanwender einige Hinweise für einen sicheren Umgang mit seinem PC.

Richtiger Umgang mit Datenträgern zur Vermeidung von Beschädigungen

- Beschriften Sie Ihre Datenträger eindeutig
- Schützen Sie Ihre Datenträger vor Schmutz und Flüssigkeiten
- Lagern Sie Ihre Datenträger trocken und kühl
- Führen Sie regelmäßige Bestandskontrollen durch

Richtiger 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 Zugangs–daten auf dem PC

Schutz vor Viren, Würmern, Abzockern und Spionen

Viren, Würmer und Trojaner sind Programme, die Daten vernichten, verändern oder auch löschen können. Sie können sich selbstständig verbreiten und reproduzieren. Abzocker und Spione sind ungebetene Gäste, die ver–trauliche Informationen die auf dem Rechner gespeichert sind ausspionieren.

- Achten Sie darauf das Ihr Betriebssystem und der Browser auf dem aktuellen Stand sind
- Setzen Sie einen Virenscanner mit einer täglichen Aktualisierung auf dem PC ein
- Setzen Sie eine Anti–Spysoftware auf dem PC ein
- Aktivieren Sie den Makro–Virenschutz der Anwen–dungsprogramme und beachten Sie die Warnmel–dungen
- Wählen Sie die höchste Stufe der Sicherheitseinstel–lungen 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 ROM‘s, Disketten mit einem Virensuchprogramm

Sicherung der Daten auf dem PC

- Die Durchführung von Wartungs– und Reparaturarbeiten sollte ausschließlich durch den Adminis–trator erfolgen
- Nehmen Sie keine Än–derungen der bestehen–den 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

Schutz der Daten vor unberechtigtem Zugriff und Manipulation am PC

- Benutzen Sie einen Bildschirmschoner mit Passwort
- Lassen Sie Ihren Arbeitsplatz nicht unbeaufsichtigt
- Schließen Sie alle Anwendungen und melden Sie sich ab bzw. schalten Sie Ihren PC beim Verlassen des Arbeitsplatzes aus
- Wenn Sie mit Wireless LAN oder VoiceOverIP arbeitet, achten Sie auf die Verschlüsselung der Kommunikation