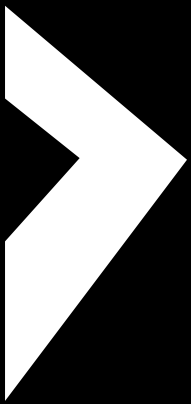
HafenCity Universität Hamburg



Empfehlungen

für den sicheren Umgang mit Informationen und IT-Geräten

Mit diesem Faltblatt möchten wir Ihnen wertvolle Tipps für einen sicheren Umgang mit Ihren Daten und IT-Geräten vermitteln (beruflich und privat). Alle Themenfelder, die bereits auf Geräten der HCU-IT berücksichtigt werden, sind mit (HCU-IT: ✓) markiert.

Warum Informationssicherheit?
Heutzutage bedrohen nicht die klassischen „Hacker", sondern immer mehr professionell organisierte Interessensgruppen die Sicherheit unserer Daten. Letztlich geht es dabei um Geld. Dies kann Zugangsdaten zum Online-Banking oder zu Ihrem Amazon-Konto betreffen, aber auch der passive Missbrauch Ihres Computers, falls dieser unbemerkt „übernommen" wurde, z. B. zur Versendung von Spam-Mails, Verteilung von Schadsoftware oder für Angriffe auf fremde Server.

Dies schadet nicht nur Ihnen, sondern auch dem Ansehen der Universität, ganz abgesehen von der Möglichkeit, dass vertrauliche Daten auf Ihrem Computer in die falschen Hände gelangen könnten.

Verwenden Sie Antiviren-Software!
Kein Rechner oder Smartphone darf ohne Antivirus-Software laufen. Bedenken Sie dabei bitte, dass Sie AV-Software nur vor bereits bekannten Schadprogrammen schützt.

Da ständig neue Schadprogramme im Umlauf sind, bringen die Hersteller meist mehrmals täglich Signaturen-Updates heraus, die Sie zeitnah einspielen sollten. (HCU-IT: ✓)

Umgang mit Passwörtern
Viele Angriffe gelingen bei simplen Passwörtern. Wählen Sie daher Ihre Passwörter sorgfältig. Sie sollten mindestens 10 Zeichen lang sein, Sonderzeichen sowie Ziffern enthalten. Teilen Sie Ihr Passwort niemandem mit. Auch ein Administrator benötigt es nicht und wird Sie nie dazu auffordern, es ihm per Mail zuzusenden oder es in ein Web-Formular einzugeben. Verwenden Sie für verschiedene Dienste jeweils eigene Passwörter. Jedes Passwort sollte regelmäßig geändert werden.

Umgang mit E-Mails, Anhängen & Links
Alle Dateien, die Ihnen unverlangt zukommen, müssen als potentiell gefährlich betrachtet werden. Gefahren lauern in aktiven Inhalten (z. B. Makros, Javascript) oder der Ausnutzung von Programmfehlern in zugehörigen Anwendungen. Fragen Sie im Zweifelsfall vor dem Öffnen einer Datei beim Absender nach, ob mit der Datei alles seine Richtigkeit hat.

E-Mail-Absenderangaben lassen sich sehr leicht fälschen! Klicken Sie nie auf den Link oder Anhang einer Spam-Mail, da dies umgehend zu einer Kompromittierung Ihres Rechners führen kann.

Verwenden Sie VPN-Verbindungen!
Wenn Sie von zuhause oder von anderswo aus über fremde Netze Daten mit dem Universitätsnetz austauschen, sollten Sie zur Verschlüsselung der Daten eine VPN-Verbindung zur HCU nutzen. Ihr PC, Laptop oder Smartphone benötigt hierfür eine Antiviren-Software mit gültigen Signaturen.

Weitere Informationen finden Sie auch unter:
www.hcu-hamburg.de/vpn

Schutz mobiler Geräte
Wenn Ihr Laptop, Smartphone, Tablet oder USB-Stick abhanden kommt und sensible Daten enthält, kann das für den „Finder" sehr vorteilhaft sein. Deshalb sollten mobile Geräte verschlüsselt oder zumindest durch ein Passwort geschützt sein. Unter der Oberfläche moderner Smartphones und Tablets befindet sich ein Betriebssystem ähnlich dem Ihres PCs, also besitzt es auch ebensolche Sicherheitslücken. Entsprechend gelten hier dieselben Regeln wie bei einem PC, z. B. was Updates betrifft.

Kabellose Netzwerke (WLANs)
WLANs bieten nicht dieselbe Sicherheit wie kabel-gebundene Netzwerke, deshalb ist eine Verschlüsselung der Übertragung notwendig. Nutzen Sie das an der HCU bereitgestellte WLAN „eduroam", so ist die Datenverschlüsselung implizit gegeben. Wenn Sie zuhause WLAN nutzen, sollten Sie die beste Verschlüsselung (derzeit WPA2/AES) einstellen. (HCU-IT: ✓)

Cloud-Nutzung
Es ist sehr einfach und bequem, Daten bei Anbietern von Online-Speichern wie Dropbox, Skydrive, iCloud oder ähnlichen zu lagern und dann mit beliebigen Endgeräten darauf zuzugreifen. Bedenken Sie aber, dass Sie Ihre Daten dabei aus der Hand geben und oft keine Einflussmöglichkeiten haben, wo Ihre Daten lagern und wer darauf Zugriff hat. Sensible Daten sollten Sie daher nicht in der Cloud speichern.

Spielen Sie Updates der Hersteller ein!
In vielen Fällen werden Rechner gekapert, indem bestehende Fehler in Programmen von Hackern für deren Zwecke genutzt werden. Deshalb ist es wichtig, die Fehlerkorrekturen der Programmhersteller (Updates oder auch Patches genannt) zeitnah einzuspielen.

Da derzeit Webbrowser und deren Hilfsprogramme (z. B. Flash, Adobe Reader, Java) beliebte Opfer sind, sollten Sie auch diese immer auf dem aktuellen Stand halten. (HCU-IT: ✓)

Verwenden Sie eine Firewall!
Eine Firewall, korrekt konfiguriert, schützt Ihren Rechner vor unerwünschten oder sogar gefährlichen Netzwerkverbindungen. Die Firewall kann ein als eigens dafür vorgesehenes Gerät im Netz oder eine „Personal Firewall" sein, die auf Ihrem Rechner läuft. Alle modernen Betriebssysteme (Windows, Mac-OS-X, Linux) bringen eine solche Personal Firewall schon mit. Erbringt Ihr Rechner keine Dienste im Netz (wie z. B. freigegebene Laufwerke oder Drucker), sollte die Firewall alle eingehenden Verbindungen abweisen. (HCU-IT: ✓)

Zugangsschutz zu Büro und PC
Denken Sie immer daran, Ihr Arbeitszimmer selbst bei kurzer Abwesenheit abzuschließen, einen Bildschirmschoner mit Passwortschutz einzustellen und Ihren Rechner zu sperren. Ansonsten kann sich jemand unbefugt Zugang zu vertraulichen Informationen verschaffen, Daten löschen oder Schadsoftware installieren, die Sie anschließend ausspioniert.

HafenCity Universität Hamburg
Henning-Voscherau-Platz 1
20457 Hamburg

Telefon +49 (0)40 - 42827-5354, -5355
Email: infothek@hcu-hamburg.de
https://www.hcu-hamburg.de

Informationssicherheits- und stellv. Datenschutzbeauftragter: Dr. Christian Paulsen

Funktionspostfach Informationssicherheit:
hcu-informationssicherheit@vw.hcu-hamburg.de

Funktionspostfach Datenschutz:
hcu-datenschutz@vw.hcu-hamburg.de