Handlungsempfehlung der Goethe-Universität Frankfurt zur Nutzung von Internetdiensten

Diese Handlungsempfehlung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt die sichere Nutzung von Internetdiensten. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung[1], werden durch diese Handlungsempfehlung nicht berührt.

In unserer modernen Welt ist das Leben ohne Internet kaum mehr vorstellbar. Nahezu alle wichtigen Informationen finden sich heute im „Web“, das mit seinen reichhaltigen Angeboten zum „Surfen“ genutzt wird. Wichtig zu berücksichtigen ist, dass die Internetnutzung nur unter Beachtung des geltenden Rechts zulässig ist, insbesondere der persönlichkeitsrechtlichen, datenschutzrechtlichen, urheberrechtlichen und strafrechtlichen Vorschriften.

Das Sicherheits-Management-Team (SMT) der Goethe-Universität empfiehlt folgende Maßnahmen, um die Sicherheit beim Surfen im Internet zu erhöhen:

1) Schutzprogramme

   - Stellen Sie sicher, dass die **interne Firewall** auf Ihrem PC aktiviert ist.

   - Installieren und aktivieren Sie ein **Anti-Virenprogramm** auf Ihrem PC und aktualisieren Sie dieses regelmäßig. Das Hochschulrechenzentrum (HRZ) bietet allen Angehörigen der Goethe-Universität einen kostenlosen Virenscanner zum Herunterladen (**Sophos** für Windows und Mac OS).

2) Sicherheitsupdates

   - Laden Sie regelmäßig **System-Updates** für Ihre Geräte herunter und installieren Sie diese. Verwenden Sie stets eine aktuelle Version des Betriebssystems und der von Ihnen installierten Programme. Spielen Sie umgehend die Sicherheitsupdates für Ihre Software, insbesondere für Ihren Webbrowser und Ihr Betriebssystem, ein. Nutzen Sie wenn möglich die Funktion zur **automatischen Aktualisierung**.

   - Deinstallieren Sie zudem **nicht benötigte Programme**. Je weniger Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche Ihres gesamten Systems.

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt

3) Accounts

- Die Nutzung von Internetdiensten sollte nur mit **Benutzerkonto** mit eingeschränkten Rechten erfolgen. Verwenden Sie keinesfalls ein Administrator-Konto!

- Gehen Sie sorgfältig mit Ihren Benutzernamen und Kennwörtern um. Dies gilt neben dem Bereich des Online-Bankings auch für Zugangsdaten, für soziale Netzwerke, Online-Shops und ähnliche Webseiten.

- Verwenden Sie **mindestens 10 bis 16 Zeichen** umfassende, sichere **Passwörter**, bestehend aus Buchstaben, Ziffern und Sonderzeichen. Speichern Sie Kennwörter, PINs und TANs oder Ihre Kreditkartendaten **niemals** auf Ihren Geräten. **Dienstliche Passwörter** dürfen **nicht** bei externen Diensten verwendet werden. Weitere Informationen finden Sie in der entsprechenden **Handlungsempfehlung „Umgang mit Passwörtern“.**

4) Software und Programme

- Laden Sie ausschließlich Programme aus **vertrauenswürdigen Quellen** herunter (bevorzugt Webseiten der Softwarehersteller).

- Achten Sie beim Installieren von Programmen und Software auf versteckte Softwarekomponenten.

5) Surfen im Internet

- Die **Eingabe von schutzwürdigen Daten** darf nur mit verschlüsselten Verbindungen (**https**) erfolgen. Haben Sie hierbei ein Augenmerk auf „https“ in der Adresszeile und ein geschlossenes Schloss-Symbol in der Statuszeile des Browsers „Firefox“.

- Die **Warnungshinweise des Webbrowsers** bezüglich der Gültigkeit und Vertrauenswürdigkeit des Zertifikats sollen beachtet werden.

- **Digitale Zertifikate** bescheinigen die Vertrauenswürdigkeit von Kommunikationspartnern im Internet.

- Surfen Sie **mit gesundem Menschenverstand**. Vertrauen Sie Meldungen, Nachrichten und Aufforderungen nicht blind. Klicken Sie nicht auf jedes Angebot, auch wenn es noch so verlockend klingt. Denn auch im Internet gibt es nichts umsonst. Viele Anbieter, die mit Preisen und Belohnungen locken, wollen nur an Ihre Daten.

6) WLAN

- WLAN-Verbindungen sollten nicht bedenkenlos genutzt werden, da diese nicht immer eine sichere, verschlüsselte Verbindung zur Verfügung stellen. Gerade beim Umgang mit

sensiblen Daten (z. B. Online-Banking, Shopping etc.) ist eine **verschlüsselte Verbindung** unerlässlich.

- **Vermeiden** Sie **Online-Banking** in Internetcafés und an öffentlichen Terminals bzw. Orten. Tippen Sie dort generell **keine Passwörter** bei der Internetnutzung ein. Wer Bankgeschäfte per Handy erledigt, sollte sich jedoch nicht die TAN auf dasselbe Gerät schicken lassen.

- Nutzen Sie am besten eine VPN-Verbindung. Das Hochschulrechenzentrum (HRZ) bietet eine kostenlose VPN-Lösung für alle Universitätsangehörigen. Weitere Informationen finden Sie unter: https://www.rz.uni-frankfurt.de/vpn

7) **Flash** ist eine veraltete Technologie und oft ein Einfallstor für Schadsoftware. Deinstallieren Sie den Flash-Player oder stellen Sie zumindest Ihren Webbrowser so ein, dass vertrauenswürdige Flash-Inhalte zum Anzeigen einzeln per Mausklick aktiviert werden müssen.

8) **Löschen** Sie **Cookies und Flash-Cookies** regelmäßig, am besten nach jeder Sitzung. Das automatisierte Löschen kann oftmals im Browser unter Einstellungen ausgewählt werden.

9) Seien Sie achtsam bei E-Mails mit unbekannten Anhängen. **Löschen Sie verdächtige E-Mails sofort** und ohne sie zu öffnen.

10) Erstellen Sie regelmäßig **Sicherungskopien** Ihrer Dateien auf externen Medien wie zum Beispiel externen Festplatten bzw. USB-Sticks, die nur für diesen Zweck eingesetzt werden, um einem eventuellen Datenverlust aufgrund einer Infektion vorzubeugen.

11) Bei Fragen können Sie sich an Ihren zuständigen IT-Support bzw. an Ihre/n IT-Sicherheitsbeauftragte/n wenden.

Informationsquellen

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) der Goethe-Universität
  https://www.uni-frankfurt.de/smt

- Goethe-Universität Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) der Goethe-Universität
  https://www.uni-frankfurt.de/hrz/it-sicherheit