Handlungsempfehlungen des Sicherheitsmanagement-Teams (SMT) der Goethe-Universität Frankfurt zu Nutzung von Online- und Internetdiensten

IMPRESSUM
IT-Sicherheitsmanagement-Team (SMT)
Goethe-Universität Frankfurt am Main
Theodor-W.-Adorno-Platz 1, PA-Gebäude
60323 Frankfurt am Main
smt@uni-frankfurt.de
https://www.uni-frankfurt.de/smt

Stand: April 2020

Inhalt

Handlungsempfehlung 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.

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

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

- 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.

Handlungsempfehlung zur Nutzung von E-Mail-Diensten

Diese Handlungsempfehlung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt die dienstliche Nutzung von E-Mail-Diensten. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung[2], werden durch diese Handlungsempfehlung nicht berührt.

Sowohl beruflich als auch privat ist der E-Mail-Dienst ein viel genutztes Kommunikationsmittel. E-Mails beinhalten oft nicht nur Text, sondern auch Links zu Webseiten und Downloads sowie Anhänge wie Bilder und Dokumente. Dadurch entstehen aber auch Risiken bei der E-Mail-Kommunikation. Angreifer und Kriminelle nutzen die Neugier der Menschen aus, um Schadsoftware per E-Mail zu verbreiten und an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern heranzukommen.

Bei der Nutzung von E-Mail-Diensten sind folgende Regeln des Sicherheits-Management-Teams (SMT) der Goethe-Universität zu beachten:

1) Für **dienstliche Belange** muss die dienstliche E-Mail-Adresse der Goethe-Universität Frankfurt zur elektronischen Kommunikation genutzt werden, sowohl als Empfangs- als auch als Absender-Adresse.

2) Die **automatische Weiterleitung** von dienstlichen E-Mails an E-Mail-Adressen externer Mail-Systeme, die nicht von der Goethe-Universität Frankfurt betrieben werden, ist **nicht zulässig**. Dienstliche Nutzung **externer E-Mail-Adressen** muss vom behördlichen **Datenschutzbeauftragten** der Goethe-Universität genehmigt werden (dsb@uni-frankfurt.de).

3) **Dienstliche E-Mail-Adressen** sollten **nicht** zur Nutzung **privater externer Dienstleistungen** (z. B. soziale Netzwerke, Online Shopping usw.) verwendet werden.

4) **Studierenden** wird aus Sicherheitsgründen empfohlen, die **Uni-Mail-Accounts** zur elektronischen Kommunikation mit Angehörigen der Universität zu verwenden.

5) Alle Beschäftigten der Goethe-Universität Frankfurt sollen – soweit möglich – Studierende nur per Uni-Mail-Adressen (**@xxx.uni-frankfurt.de-Adressen**) kontaktieren (mit Ausnahme von Antworten auf ihre E-Mails).

6) Verseuchte **E-Mail-Anhänge** und **Links** sind einer der häufigsten Wege, Schadsoftware in Computer einzuschleusen. Deshalb gilt stets erhöhte Aufmerksamkeit vor dem Klicken auf

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

einen Link bzw. vor dem Öffnen eines Anhangs. Absender, Betreff und E-Mail-Text sollten stimmig und plausibel sein.

7) **Bewerbungen** bzw. **Bewerbungsunterlagen** dürfen ausschließlich im **PDF-Format** eingereicht werden. Im Falle von Zip-Dateien oder Word-Dokumenten können Sie die Bewerber/innen dazu auffordern, Bewerbungen im PDF-Format noch einmal einzureichen.

8) **Digitale Zertifikate** bescheinigen die Vertrauenswürdigkeit von Kommunikationspartnern. Achten Sie auf Gültigkeit und Vertrauenswürdigkeit des Zertifikats, wenn Sie eine signierte E-Mail erhalten.

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

Handlungsempfehlung zum Umgang mit Passwörtern

Diese Handlungsempfehlung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt den sicheren Umgang mit Passwörtern. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung[3], werden durch diese Handlungsempfehlung nicht berührt.

Die Daten in einem System müssen geschützt sein und nur berechtigte Personen dürfen darauf zugreifen. Dies kann mithilfe persönlicher Chipkarten, durch Prüfung biometrischer Eigenschaften (z. B. Fingerabdruck) oder durch Eingabe einer Benutzerkennung und eines Passwortes erfolgen. Kartengestützte und biometrische Anmeldeverfahren gewinnen zwar immer mehr an Bedeutung; in der Praxis dominiert jedoch bislang die Anmeldung mit Benutzerkennung und Passwort. Dieses Merkblatt stellt dar, wie sich ein möglichst sicherer Passwortschutz realisieren lässt.

Erfährt jemand Ihre Benutzerkennung und Ihr Passwort, so kann er sich damit unter Ihrem Namen anmelden und auf Ihre Daten und Programme zugreifen, die nicht für ihn bestimmt sind. Da Benutzerkennungen vielfach nicht geheim sind, kommt der Geheimhaltung der persönlichen Passwörter die entscheidende Rolle zu.

Das Sicherheits-Management-Team (SMT) der Goethe-Universität empfiehlt folgende Regeln für die Wahl von Passwörtern:

1) Es wird eine Passwortlänge von **16 Zeichen** empfohlen, mindestens 10 Zeichen sollten es aber auf jeden Fall sein.

2) Das Passwort sollte Groß-/Kleinbuchstaben, Zahlen und möglichst **Sonderzeichen** enthalten.

3) Um ein Passwort der nötigen Länge zu finden, das man sich auch leicht merken kann, können beispielsweise zwei oder mehr ***zusammenhangslose (!)*** Wörter aneinandergehängt werden, wenn zufällige Zeichen zwischen sie gestreut werden.

4) Sofern technisch nur kürzere Passwörter möglich sind, sollte auf eine große „**Zufälligkeit**“ der Zeichen geachtet werden. Dies kann man erreichen, indem man sich einen Satz merkt, die Anfangsbuchstaben der Worte nimmt und an passender Stelle noch Sonderzeichen einstreut.

5) Das Passwort darf nicht leicht zu erraten sein, wie zum Beispiel Benutzername, Vor- oder Nachname, Kfz-Kennzeichen, Geburtsdatum.

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

6) Das Passwort muss **geheim** gehalten und sollte regelmäßig geändert werden. **Dienstliche Passwörter** dürfen **nicht** bei externen Diensten verwendet werden.

7) Ein Passwort sollte immer nur an einer Stelle benutzt werden. Leicht merken kann man sich diese Passwörter dennoch, wenn man z. B. einige wechselnde Zeichen vor eine häufiger genutzte Zeichenkette stellt, also beispielsweise „`GUHier2Mond%Kachel`“, „`1aHier2Mond%Kachel`“ ...

8) **Mail-Zugänge** müssen besonders gut geschützt werden, da darüber alle anderen Passwörter geändert werden können. Hier dürfen also keinesfalls Passwörter verwendet werden, die auch an anderer Stelle genutzt werden.

9) **Beispiele** für Passwörter sind (verwenden Sie diese Beispiele auf keinen Fall als Passwort, diese kann man nämlich jetzt einfach ausprobieren …):

   ```
   Hier2Mond%Kachel
   6uybi+sY
   msJ$DR8Ttx
   …
   ```

10) „**Passwort-Manage**r”, also Programme, die Passwörter speichern, helfen, viele verschiedene Passwörter zu nutzen. Die Passwort-Manager der Webbrowser sollten nur genutzt werden, wenn diese mit einem eigenen Passwort geschützt werden können. Externe Programme sind eher zu empfehlen.

11) Ein **Passwortwechsel** ist sofort durchzuführen, wenn der Verdacht besteht, dass das Passwort unautorisierten Personen bekannt geworden ist oder wenn der Verdacht auf eine **System-Kompromittierung** besteht. In diesem Fall wenden Sie sich unverzüglich an den zuständigen Administrator bzw. IT-Sicherheitsbeauftragten. Das **HRZ-Passwort** können Sie unter diesem Link ändern: https://kartenservice.uni-frankfurt.de/mitarbeitercard/password

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

Handlungsempfehlung zur Auslagerung von Daten in die Cloud

Diese Handlungsempfehlung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt die dienstliche Nutzung von Cloud-Diensten. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung[4], werden durch diese Handlungsempfehlung nicht berührt.

Vor dem Hintergrund der sich immer mehr auflösenden Trennung von privaten und dienstlichen Belangen, speziell im IT-Umfeld, soll diese Richtlinie zur Sensibilisierung gegenüber den potenziellen Risiken beitragen und entsprechende Handlungsanleitungen geben.

Cloud-Dienste werden in vielen Bereichen seit vielen Jahren bewusst oder unbewusst genutzt. Hierbei ist zu beachten, dass diese meist „kostenlosen" Dienste indirekt durch Daten der Nutzenden „bezahlt" werden. Dies kann z. B. bis zur Abtretung der Rechte an den in Cloudspeichern abgelegten Daten führen. Daher ist die Speicherung von Daten in öffentlichen Clouds zu vermeiden.

Zur Speicherung von Daten in der Cloud sind folgende Regeln des Sicherheits-Management-Teams (SMT) der Goethe-Universität zu beachten:

1) Als Cloud-Dienst zur Online-Speicherung von Dateien wird u. a. die Sync-&-Share-Lösung **Hessenbox** (https://hessenbox.uni-frankfurt.de) empfohlen. Diese wird von der Goethe-Universität Frankfurt betrieben und kostenlos angeboten. Die Hessenbox ist als zugelassenes IT-Verfahren angemeldet. Weitere Informationen finden Sie unter diesem Link: https://www.rz.uni-frankfurt.de/hessenbox

2) In der Hessenbox abgelegte Daten müssen **je nach Schutzbedarf** seitens des/der Dateneigentümer/s/in verschlüsselt werden. Hierzu können frei verfügbare Werkzeuge verwendet werden:

   - **Dateien in einer Datei**
     7-Zip (https://www.7-zip.org/)

   - **Dateien in einem Container**
     VeraCrypt (https://www.veracrypt.fr/en/Home.html)
     Cryptomator (https://cryptomator.org/de/)

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

3) Zur Sicherheit wird empfohlen, Cloud-Dienste nur über deren **Webseiten** zu nutzen und auf Apps und andere Programme zu verzichten. Wenn die Nutzung von Apps oder anderen Programmen zur Synchronisation von Daten nicht vermeidbar ist, achten Sie darauf, dass nur die **benötigten Verzeichnisse** synchronisiert werden.

4) Selbstverständlich muss auch genau beachtet werden, an welchen Personenkreis **Freigaben** erfolgen.

5) Cloud-Dienste wie Dropbox, Google Drive, iCloud, OneDrive, Amazon Drive usw. sollten nur benutzt werden, **wenn dies unvermeidbar ist**. Hierbei sind dann einige weitere Punkte zu beachten:

   - Die dienstliche Nutzung externer Cloud-Dienste muss vom behördlichen **Datenschutzbeauftragten** der Goethe-Universität genehmigt werden (dsb@uni-frankfurt.de).

   - **Verboten** ist die Nutzung externer Cloud-Dienste für personenbezogene oder urheberrechtlich geschützte Daten.

   - Eine **Geheimhaltung** kann bei externen Anbietern **nicht gewährleistet** werden. Daten sollten daher vor der Speicherung in externen Diensten verschlüsselt werden.

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

Handlungsempfehlung zur Nutzung von mobilen Geräten

Diese Handlungsempfehlung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt die sichere Nutzung von mobilen Geräten. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung[5], werden durch diese Handlungsempfehlung nicht berührt.

Mittlerweile entsprechen die mobilen, internetfähigen Geräte kleinen Computern, mit denen gearbeitet und kommuniziert wird und auf denen vertrauliche Daten gespeichert werden. Dadurch gelten für sie mindestens die gleichen Sicherheitsanforderungen wie für stationäre Computer.

Die Sicherheit spielt im Grunde sogar eine noch größere Rolle, denn die Möglichkeit, die Geräte immer und überall dabei zu haben und sie ständig mit dem Internet zu verbinden, birgt zusätzliches Gefahrenpotenzial. Die dienstliche Nutzung von privaten Geräten ist nicht nur praktisch, sondern stellt zusätzliche Anforderungen an die sichere Verwendung der Geräte.

Das Sicherheits-Management-Team (SMT) der Goethe-Universität empfiehlt folgende Maßnahmen für die Informationssicherheit mobiler Geräte:

1) Achten Sie **beim Kauf** von mobilen Geräten auf Aktualität des Betriebssystems sowie **Verfügbarkeit von Updates**.

2) Sorgen Sie für einen **Basisschutz** und führen Sie regelmäßig Sicherheitsupdates durch.
   - Halten Sie das Betriebssystem und sämtliche installierte Software und Apps mit **Sicherheitsupdates** immer auf dem neuesten Stand. Viele Angriffe zielen auf bekannte Schwachstellen, die erst durch Updates der Hersteller geschlossen werden. Aktivieren Sie daher die **automatische Update-Funktion**, damit Sicherheitsupdates direkt nach dem Erscheinen eingespielt werden.

3) Installieren Sie Apps nur **aus vertrauenswürdigen Quellen** und prüfen Sie die Zugriffsberechtigungen.

   - Informieren Sie sich vor Installation einer App, wenn Ihnen der Anbieter nicht bekannt ist. Eine kurze Suche im Internet reicht meistens aus, um sich zu informieren. Entfernen Sie **veraltete Anwendungen** oder solche, die Sie nicht mehr nutzen. Denn jede zusätzliche App ist eine mögliche Sicherheitslücke.
   - Viele Apps räumen sich ohne erkennbaren Grund umfassende Rechte ein. Ein Zugriff auf beispielsweise Standortdaten, Adressbuch oder den Telefonstatus ist nicht bei jeder App

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

notwendig. Prüfen Sie daher kritisch, ob die **Zugriffsrechte** zum Erfüllen der Funktionalität wirklich notwendig sind.

4) Nutzen Sie **Sperrcodes und Passwörter**.
   - Der Zugriff auf mobile Geräte und deren Anwendungen muss durch Schutzvorkehrungen wie Passwort, PIN usw. abgesichert werden.

5) Aktivieren Sie Schnittstellen nur bei Bedarf und sichern Sie diese.
   - Deaktivieren Sie Drahtlosschnittstellen, wie **Bluetooth oder NFC**, wenn Sie diese nicht benötigen. So ist Ihr Gerät weniger anfällig für Cyber-Angriffe.

6) Schließen Sie Ihr mobiles Gerät nur an **vertrauenswürdige Rechner** an.

7) Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht.
   - Öffentliche WLAN- Hotspots 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.

   - 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

8) Lassen Sie Ihr Gerät nicht aus den Augen.
   - Um das Gerät vor unbefugtem Zugriff und Manipulation zu schützen, sollten Sie Ihr Smartphone **niemals unbeobachtet lassen oder verleihen**. Verlorene oder gestohlene dienstliche Geräte müssen dem zuständigen IT-Support gemeldet werden.

9) Surfen Sie mit gesundem Menschenverstand.
   - Bewahren Sie sich eine gesunde Skepsis, welcher Empfehlung beispielsweise für eine App Sie folgen wollen, was Sie von wo installieren beziehungsweise worauf Sie alles klicken. Nicht alles hält letztlich, was es verspricht, und leere Versprechungen werden gerne genutzt, um Schadsoftware auf dem Gerät zu installieren.

10) Schützen Sie Ihre Daten.
   - Nutzen Sie die Funktionen zur **Datenverschlüsselung**, wenn vorhanden, oder verschlüsseln Sie sensible Daten selbst mit einer Verschlüsselungssoftware.

   - Erstellen Sie regelmäßig **Sicherungskopien**.

11) Prüfen Sie unbekannte Rufnummern vor Rückruf.

- Aktuelle Informationen zu missbräuchlich genutzten Rufnummern finden Sie auf der Webseite der Bundesnetzagentur. Lassen Sie bei Bedarf unerwünschte Rufnummern zu Mehrwertdiensten von Ihrem Netzbetreiber sperren.

  https://www.bundesnetzagentur.de/Rufnummernmissbrauch

12) Löschen Sie alle Speicher, bevor Sie das Gerät verkaufen oder entsorgen.

- Wenn Sie nicht möchten, dass Ihre gespeicherten Daten beim Verkauf oder bei der Entsorgung Ihres Gerätes in falsche Hände geraten, dann sollten alle Datenspeicher (**interner Speicher und SD-Karten**) sicher gelöscht werden. Die SIM-Karte und ggf. die SD-Karten sollten Sie entfernen und – falls Sie diese nicht weiterverwenden wollen – vernichten.

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

Abkürzungen

App: Application (Applikation, Anwendungssoftware)

BSI: Bundesamt für Sicherheit in der Informationstechnik

CEO: Chief Executive Officer (Geschäftsführer)

CERT: Computer Emergency Response Team

DFN: Deutsches Forschungsnetz

GPS: Global Positioning System

HRZ: Hochschulrechenzentrum

HTTPS: HyperText Transfer Protocol Secure
(Sicheres Hypertext-Übertragungsprotokoll)

IT: Information Technology (Informationstechnik)

IuK: Nutzungsordnung für Informationsverarbeitungs- und Kommunikationsinfrastruktur

NFC: Near Field Communication (Nahfeldkommunikation)

OS: Operating System (Betriebssystem)

PC: Personal Computer (Einzelplatzrechner)

PIN: Personal Identification Number (Persönliche Identifikationsnummer)

SD-Karte: Secure Digital Memory Card (Sichere Digitale Speicherkarte)

SMT: Security Management Team (Sicherheitsmanagement-Team)

USB: Universal Serial Bus (Serielles Bussystem)

VPN: Virtual Private Network (Virtuelles Privates Netzwerk)

WLAN: Wireless Local Area Network (Drahtloses Lokales Netzwerk)

Informationsquellen

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

Hessen Cyber Competence Center (Hessen3C)
https://innen.hessen.de/sicherheit/hessen3c

Verein zur Förderung eines Deutschen Forschungsnetzes (DFN-Verein)
https://www.dfn.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