Herzlich Willkommen!

Über den Button können Sie weiter navigieren.

Achten Sie auch auf anklickbare Elemente auf den jeweiligen Seiten, um alle Informationen zu erfassen.

weiter

Inhalte

Risiken & Schutzmaßnahmen im Netz

- Phishing
- Sicheres Surfen & Arbeiten
- Passwörter
- Datenaustausch per USB
- Datenaustausch per Cloud
- Zutrittsberechtigung
- Datenentsorgung

Reaktion beim Sicherheitsvorfall

- Definition
- Zuständigkeiten
- Verhaltensweisen

Handreichungen & Downloads

zurück

weiter

Risiken & Schutzmaßnahmen im Netz

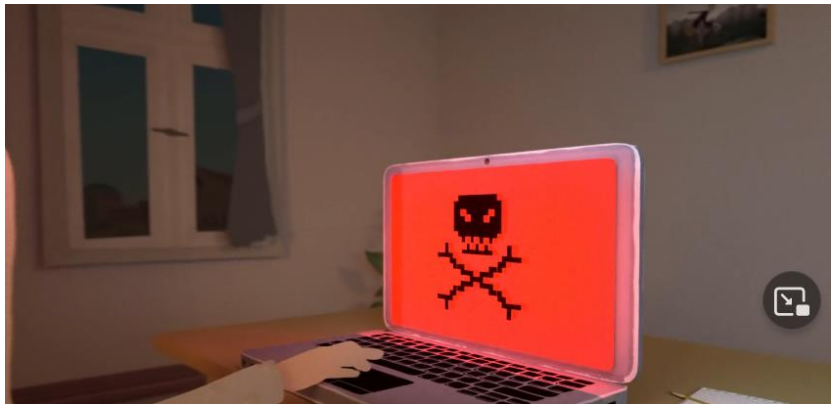
- **Phishing**
- Sicheres Surfen & Arbeiten
- Passwörter
- Datenaustausch per USB
- Datenaustausch per Cloud
- Zutrittsberechtigung
- Datenentsorgung

zurück

weiter

Phishing

Einer der größten Gefahren im digitalen Schriftverkehr ist das sogenannte *Abfischen* von Daten.



https://wiki.secuso.org/videos/nophish/video-1-anhaenge-2020-deutsch-precredits-001_recode.mp4

- Cyber-Kriminelle verschicken betrügerische Nachrichten per E-Mail, über Messenger oder über soziale Netzwerke. Sie fordern Nutzerinnen und Nutzer dazu auf, vertrauliche Informationen wie Passwörter, Zugangsdaten oder Kreditkartennummern preiszugeben. Angeschriebene sollen auf einen Link klicken.
- Die Gefahr: Die angegebenen Links führen auf gefälschte Internetseiten, auf denen die Daten abgegriffen werden. Die Nachrichten wirken täuschend echt, die Absender seriös. Viele Empfänger schöpfen daher keinen Verdacht und geben ihre Daten den Kriminellen preis.

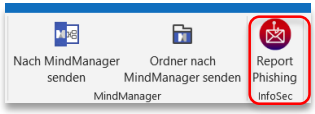
zurück

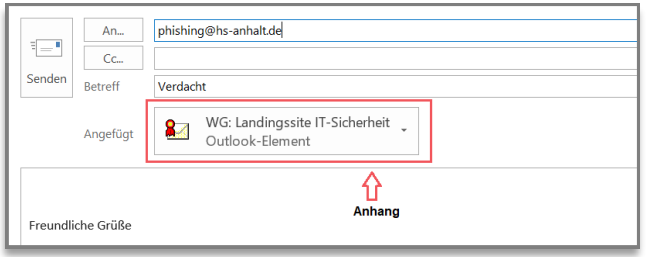
weiter

E-Mail - SPAM und Phishing melden

- Melden Sie verdächtige E-Mails an **phishing@hs-anhalt.de**.
- Bitte leiten Sie die **E-Mail ausschließlich als E-Mail-Anhang** weiter.

Dazu ziehen Sie die verdächtige Mail aus ihrem E-Mail Programm (bspw. Outlook) in eine neue E-Mail-Vorlage (Drag & Drop) und versenden Sie sie an die entsprechende Adresse oder verwenden Sie den Phishing-Meldebutton.





Alternativ verfahren Sie im Programm Outlook unter Start und über das Symbol **Als Anlage weiterleiten** rechts neben Weiterleiten. Gegebenenfalls finden Sie dies auch bei den Antwort- und Weiterleiten-Funktionen unter **Weitere**.

zurück

weiter

Phishing – Wie Sie sich schützen können

Seien Sie skeptisch bei E-Mails unbekannter Absender. Ihre Bank, Diensteanbieter oder Behörden bitten niemals per E-Mail darum, persönliche Daten wie Passwörter über einen Link zu ändern.

Verwenden Sie für die diversen Account-Zugänge möglichst eine Zwei-Faktor-Authentisierung. Durch die zweite Stufe der Identifizierung können Kriminelle selbst dann nicht auf Ihre Daten zugreifen, wenn sie bereits Ihr Passwort erbeutet haben.

Bei Zweifeln lassen Sie sich die Echtheit einer E-Mail vom Absender telefonisch bestätigen. Nutzen Sie dafür nicht die Telefonnummer aus der E-Mail, sondern suchen Sie diese selbst, bspw. aus dem Personalverzeichnis heraus.

Achten Sie auf die Verwendung von sogenannten Nutzer-Zertifikaten. Sie erkennen Sie im Outlook z. B. an einem roten Siegel. Das bedeutet, dass die Identität der absendenden Person einwandfrei geklärt ist.

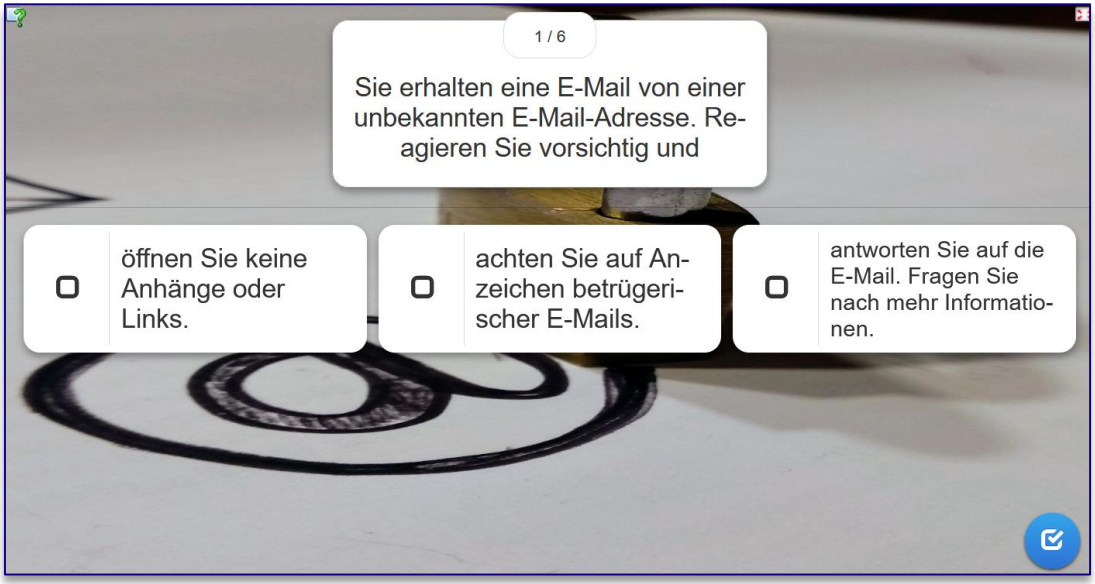
Vorsicht bei Anhängen mit Formaten wie .exe oder .scr. Diese können Schadsoftware direkt auf Ihr Gerät laden. Manchmal werden Nutzer oder Nutzerinnen auch durch Doppelendungen wie Dokument .pdf.exe in die Irre geführt. Auch Dateiendungen wie .bat, .com, .cmd, .pif, .hta können Schadsoftware beinhalten.

zurück

weiter

Phishing –Quiz

Klicken Sie auf nachfolgenden **Link** oder das **Bild** um ihr Wissen zu testen



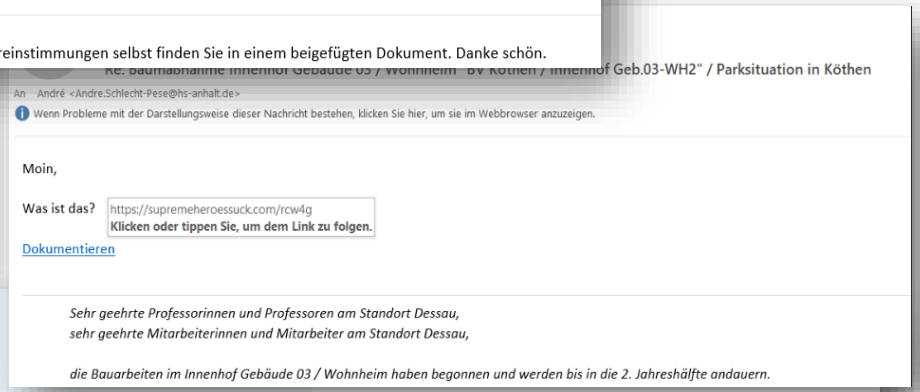
https://learningapps.org/17800388

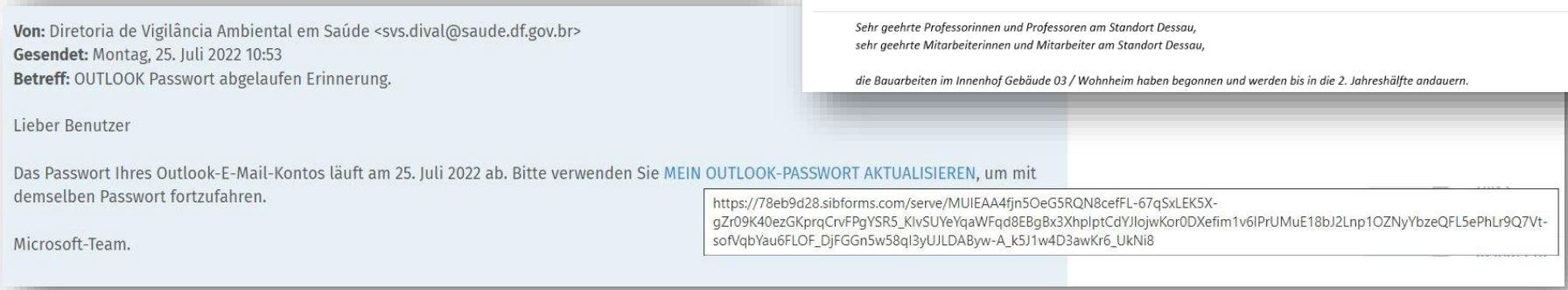
zurück

weiter

HOCHSCHULE ANHALT University of Applied Sciences

Phishing – Beispiele





zurück

weiter

Risiken & Schutzmaßnahmen im Netz

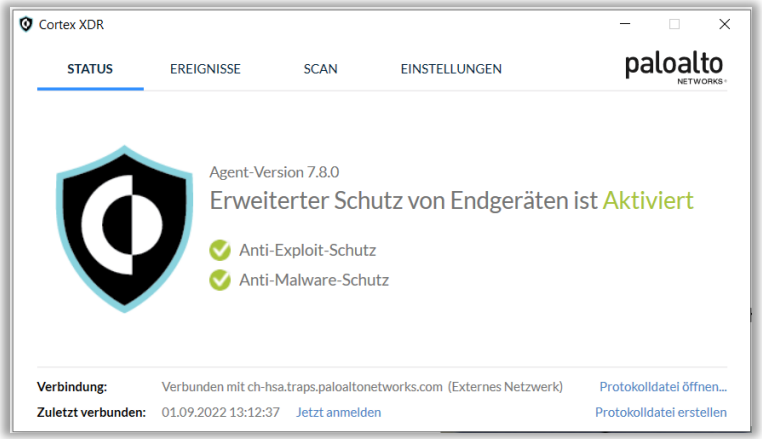
- Phishing
- **Sicheres Surfen & Arbeiten**
- Passwörter
- Datenaustausch per USB
- Datenaustausch per Cloud
- Zutrittsberechtigung
- Datenentsorgung

zurück

weiter

Sicheres Surfen & Arbeiten

Zur Gefahrenreduktion sind folgende Maßnahmen empfohlen



- Surfen Sie auf Seiten mit gültigem Zertifikat (***https*** bzw. geschlossenes „Schloss-Symbol“)
- Führen Sie alle notwendigen Updates durch
- Verändern Sie nicht selbständig die Einstellungen an der Betriebssystem-Firewall
- Verwenden Sie eine Anti-Malware-Anwendung (z. B. PaloAlto Cortex XDR)

zurück

weiter

Sicheres Surfen & Arbeiten

- Beschaffen Sie Software ausschließlich über das **ISC** oder den Admin der Hochschule
- Führen Sie keine eigenständigen Downloads und keine eigenständige Installation von Software über Webseiten durch
- Benutzen Sie eine aktuelle Version von ihrem Browser
- Verwenden Sie sichere Suchmaschinen wie **Startpage** oder **Metager**
- Seien Sie aufmerksam beim Öffnen von E-Mails

zurück

weiter

Risiken & Schutzmaßnahmen im Netz

- Phishing
- Sicheres Surfen & Arbeiten
- **Passwörter**
- Datenaustausch per USB
- Datenaustausch per Cloud
- Zutrittsberechtigung
- Datenentsorgung

zurück

weiter

Passwörter

Ein gutes **Passwort** ist wichtig, denn niemand sollte auf ihre **Accounts** und **Daten zugreifen** können oder diese mitlesen.

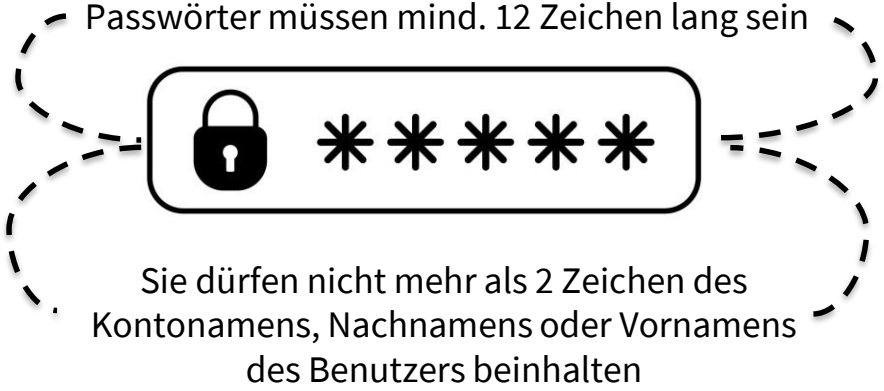
Bei der Wahl eines Passwortes sind Ihrer Kreativität **keine Grenzen** gesetzt. Verwenden Sie für ein starkes Passwort mind. 10 Zeichen, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Wie Sie sich ein gutes Passwort erstellen und merken können, sehen Sie auf dem **Bild** rechts.

zurück

weiter

Passwörter

Seit Mai 2022 gelten an der Hochschule Anhalt nachfolgende Passwortbestimmungen. Passwörter sollten entsprechend erstellt und geändert werden.



Passwörter dürfen enthalten

- Großbuchstaben der englischen Sprache (A bis Z)
- Kleinbuchstaben der englischen Sprache (a bis z)
- Ziffern zur Basis 10 (0 bis 9)
- Sonderzeichen, z. B. !@#$%&_-+=(){}[]<>,.?

Passwörter dürfen <u>nicht</u> enthalten

- die Zeichen :;äöüÄÖÜß sind nicht erlaubt
- das Passwort darf keine Leerzeichen enthalten

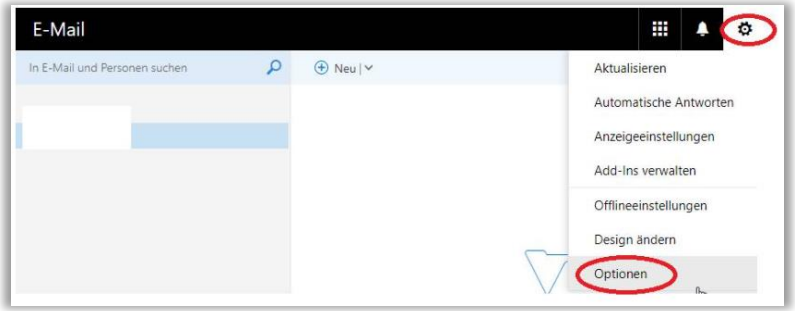
zurück

weiter

Passwörter

Müssen Sie ein Passwort ändern, haben Sie folgende Möglichkeiten

Webmail-Formular **https://mail.hs-anhalt.de**



Self-Service: **https://selfservice.hs-anhalt.de**

Weitere Hinweise zur Handhabung finden Sie **hier**.

Risiken & Schutzmaßnahmen im Netz

- Phishing
- Sicheres Surfen & Arbeiten
- Passwörter
- **Datenaustausch per USB**
- Datenaustausch per Cloud
- Zutrittsberechtigung
- Datenentsorgung

zurück

weiter

Datenaustausch per USB

USB-Geräte werden von vielen Menschen in Unternehmen genutzt. Sie ermöglichen einen einfachen und bequemen Austausch und Transport von Daten, können aber auch unbekannte Elemente in ein Netzwerk einbringen.

Cyberkriminelle können mit USB-Geräten auch Netze außerhalb des Internets erreichen und "bösartige" Software einschleusen. Diese sog. Malware kann auf die Daten der Benutzer zugreifen und den Angreifern, Zugang zu Tastatur und Bildschirm verschaffen, um alles zu sehen, was die Benutzer tun oder um Befehle abzusetzen, die zur Verschlüsselung von Daten führen können.

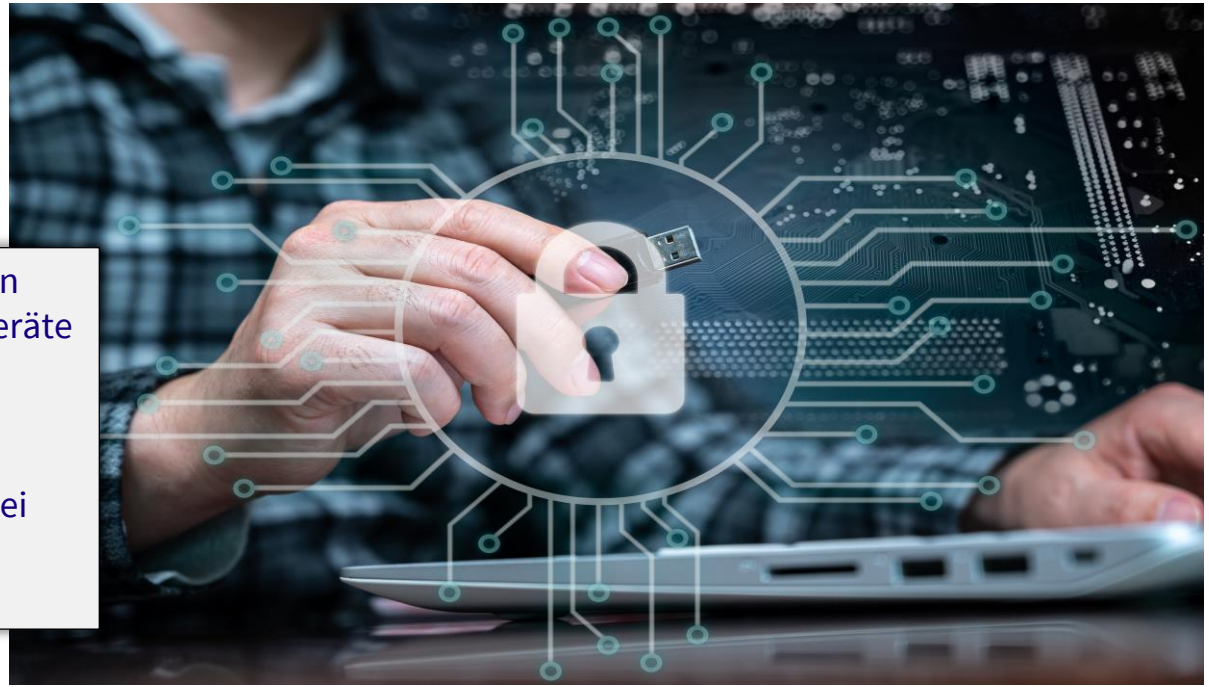
zurück

weiter

Datenaustausch per USB

!!!

- Stecken Sie keine fremden und unbekannten USB-Geräte an ihren Rechner
- Seien Sie Vorsichtig bei Werbegeschenken oder bei Fundstücken auf dem Hochschulgelände



zurück

weiter

Risiken & Schutzmaßnahmen im Netz

- Phishing
- Sicheres Surfen & Arbeiten
- Passwörter
- Datenaustausch per USB
- **Datenaustausch per Cloud**
- Zutrittsberechtigung
- Datenentsorgung

zurück

weiter

Datenaustausch per Cloud

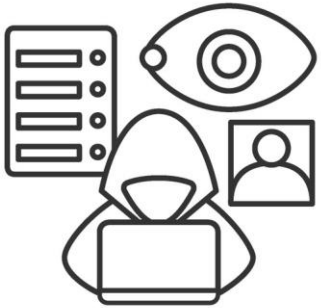
Die Cloud ist ebenfalls ein Medium, über welches Informationen bzw. Daten ausgetauscht werden können. Sie wird auch als virtueller Speicherort bezeichnet, auf den via Webbrowser geräteunabhängig, per Internet, zugegriffen werden kann.

Das interne Cloudsystem der Hochschule Anhalt heißt Nextcloud und ist auch extern über **cloud.hs-anhalt.de** erreichbar.

zurück

weiter

Datenaustausch per Cloud



Cloudsysteme bieten ein lukratives **Angriffsziel** für Cyberkriminelle, weil sie dort viele interessante Daten vermuten.

- Nutzen Sie für dienstliche Daten keine Cloud von externen Anbietern
- **Hoch vertrauliche, dienstliche Daten gehören in keine Cloud**
- Wenn Sie Dateien mit externen Partnern aus der Nextcloud heraus teilen möchten, setzen Sie ein Ablaufdatum für den Zugriff und vergeben ein Passwort
- Wie Sie die Nextcloud benutzen, erfahren Sie **hier**

zurück

weiter

Risiken & Schutzmaßnahmen im Netz

- Phishing
- Sicheres Surfen & Arbeiten
- Passwörter
- Datenaustausch per USB
- Datenaustausch per Cloud
- **Zutrittsberechtigung**
- Datenentsorgung

Zutrittsberechtigung

Angreifer können Zugriff auf die IT-Infrastruktur erhalten, indem Sie sich Zutritt zu den örtlichen Gegebenheiten verschaffen.

Dieses Angriffsmethode wird **Tailgating**, zu deutsch **Hindurchschlüpfen** genannt. Dabei meldet sich ein Mitarbeiter mit seinem Ausweis an und der Täter schleicht sich unbemerkt hinter ihm ein. Kriminelle nutzen es dazu, sich physischen Zugang zu Computersystemen und anderen sensiblen Geräten zu verschaffen.

zurück

weiter

Zutrittsberechtigung - Tailgating vermeiden

- Seien Sie wachsam, ob sich jemand unbefugt und auffällig neugierig im Bürogebäude oder auf dem Hochschulgelände bewegt.

- Seien Sie aufmerksam beim Zutritt in gesicherte Bereiche, dass nicht jemand hinter Ihnen durch die von Ihnen geöffnete Tür huschen kann!

- Halten Sie fremden Personen keine gesicherte Tür auf!

- Behalten Sie Ihre Mitarbeiterkarte im Auge, da Sie bei Verlust auch jedem Fremden Zutritt verschafft!

zurück

weiter

Risiken & Schutzmaßnahmen im Netz

- Phishing
- Sicheres Surfen & Arbeiten
- Passwörter
- Datenaustausch per USB
- Datenaustausch per Cloud
- Zutrittsberechtigung
- **Datenentsorgung**

zurück

weiter

Datenentsorgung

Sensible Informationen und Daten sind bis zu ihrer Vernichtung zu verschließen und müssen vor fremden Zugriff geschützt werden.

- Bei kleineren vertraulichen Papiermengen nutzen Sie bitte einen Aktenvernichter mit Kreuzschnitt.
- Bei einem größeren Bedarf können Sie bei der zentralen Beschaffung der Hochschule Anhalt eine Datenschutztonne anmelden.
- Wollen Sie Festplatten entsorgen, wenden Sie sich bitte an das IT-Service-Center der Hochschule, welches die physische Zerstörung vornimmt.

zurück

weiter

Reaktion beim Sicherheitsvorfall

- **Definition**
- Zuständigkeiten
- Verhaltensweisen

Sicherheitsvorfall Definition

Ein **Informationssicherheitsvorfall** ist ein/e

nicht-technischer & technischer Angriff durch nicht autorisierte Dritte (z. B. Scanner, Sniffer, DoS, unbefugter Zutritt)

Kompromittierung von Funktionen oder auch Fehlkonfigurationen (z. B. Missbrauch von Zugriffsrechten)

Kompromittierung von Informationen durch Verletzung der Sicherheit beim Schutz personenbezogener Daten durch Vernichtung, Verlust oder Veränderung, unbefugte Offenlegung

physischer Schaden (z. B. Verlust von hochschuleigener Technik)

Ausfall der (techn.) Infrastruktur wichtiger Bereiche (Zutritts-system, Netzsegment)

vermehrtes Auftreten von bösartiger Software (Malware)

Verbreitung unerwünschter Inhalte & nicht autorisierter Massen-Mailversand aus dem Hochschulnetz

zurück

weiter

Reaktion beim Sicherheitsvorfall

- Definition
- **Zuständigkeiten**
- Verhaltensweisen

Zuständigkeiten

Informationssicherheitsvorfälle können von verschiedenen Quellen gemeldet werden. Sie erfolgen durch Monitoring- und Gebäudesicherheitssysteme, Externe oder durch Hochschulangehörige wie Mitarbeitende, Studierende, Professoren, Lehrbeauftragte.

Hochschulangehörige können sich bei Vorfällen **an die jeweilige Führungskraft oder zuständigen Administrator** in ihrem Bereich **wenden**.

IT Ansprechpartner am jeweiligen Fachbereich

- Verwaltung: Christian Städtler, Friedemann Elze
- Landesstudienkolleg: Ute Lewandowski

- Fachbereich 1 / LOEL: Malte Klein
- Fachbereich 2 / WI: Frank Königsberg
- Fachbereich 3 / AFG: Nachbesetzung folgt
- Fachbereich 4 / DES: Uwe Krehan
- Fachbereich 5 / INS: Heike Hennicke, Ralf Pelzl
- Fachbereich 6 / EMW: Holger Brandt
- Fachbereich 7 / BWP: Frank Engelmann

Reaktion beim Sicherheitsvorfall

- Definition
- Zuständigkeiten
- **Verhaltensweisen**

zurück

weiter

Verhaltensweisen

Beachten Sie folgende Regeln beim Verdacht auf einen Sicherheitsvorfall

- Falls es Ihre aktuelle Arbeit am PC betrifft, stellen Sie diese bitte ein.
- Melden Sie den Vorfall unverzüglich an den zuständigen Betreuer/Admin oder wählen Sie die +49 3496 67 5500.
- Schildern Sie den Vorgang möglichst genau (Wer ruft an? Welches IT-System ist betroffen? Was wurde beobachtet? Wann ist es passiert? Wo befindet sich das IT-System?).
- Warten Sie auf weitere Anweisungen.
- Gegebenenfalls werden Sie gebeten, das IT-System vom Netzwerk zu trennen, aber eingeschaltet zu lassen.

zurück

weiter

Handreichungen & Downloads

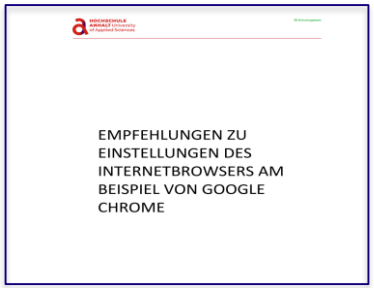
Klicken Sie für praktische **Tipps** und **Hinweise** zum Thema **Informationssicherheit** auf nachfolgende **Kacheln**

Flyer HSA

Passwortkarte

Sichere Geräte & Software

IT-Sicherheitslage Deutschland



Broschüre Browsereinstellungen

IT-Lexikon

zurück

weiter

Vielen Dank

Wir hoffen, dass wir Ihr Interesse für das Thema wecken konnten.

Wenn Sie sich für die Grundstufe anmelden möchten, schreiben Sie uns dies via Mail an **isi@hs-anhalt.de**

zurück