Die Hochschule Anhalt unterhält ein **Programm zur Aus- und Weiterbildung** der Mitarbeitenden und Professorinnen und Professoren zu den Themen Informationssicherheit und Datenschutz, welches vom ISI-Schulungsteam durchgeführt wird.

Folgenden Veranstaltungen werden angeboten:

- IT-Basisschulung
- weiterführende IT-Sicherheitsschulungen
- Workshops
- Phishing Simulationen zu Trainingszwecken
- Live Security Events

Haben Sie schon Ihr Zertifikat?

Aufgrund des gestiegenen Sicherheitsbedarfs an der Hochschule Anhalt und auch zu Ihrem persönlichen Schutz empfehlen wir Ihnen dringend die Teilnahme an der IT-Basisschulung (Onlinekurs) und am anschließenden vertiefenden Workshop.

Folgende Inhalte werden dabei vermittelt:

- Was bedeutet Informationssicherheit?
- Wie gehe ich sicher mit Informationen/Daten um?
- Was gebe ich warum, wann und wie weiter?
- Welche aktuell bekannten Gefahren und Bedrohungen gibt es?
- Wie werden Informationssicherheitsvorfälle erkannt und gemeldet?
- Wie verhalte ich mich richtig?

Nach erfolgreicher Absolvierung erhalten Sie das Grundstufen-Informationssicherheitszertifikat (GS-ISI-Zertifikat), das Sie dem Personaldezernat als Ergänzung Ihrer Qualifizierungen in der Personalakte weiterleiten können.

KONTAKT

HOCHSCHULE ANHALT University of Applied Sciences

Hochschule Anhalt
University of Applied Sciences
Bernburger Straße 55
06366 Köthen

Wir besprechen mit Ihnen gern neue und bekannte Themen der Informationssicherheit und des Datenschutzes!

Kontakt
Informationssicherheit (ISI) der Hochschule Anhalt

Informationssicherheitsbeauftragte/r
Telefon: +49 (0) 3496 67 5415
it-sicherheit@hs-anhalt.de

Unter folgendem Link erhalten Sie u.a. aktuelle Informationen, weitere Sicherheitstipps und die Möglichkeit zur Einsicht, wann welche Schulungen durchgeführt werden:

www.hs-anhalt.de
/isi-schulungen

HOCHSCHULE ANHALT University of Applied Sciences

Grundregeln für Informationssicherheit

Wie Sie sich an Ihrem Arbeitsplatz und in Ihrem privaten Umfeld vor Cyberangriffen schützen können

Das ISI-Schulungsteam informiert

Stand 01/2023

www.hs-anhalt.de

Wachsames Verhalten beugt Cyberangriffen vor

Das ISI-Schulungsteam der Hochschule Anhalt hilft Ihnen dabei, sich bestmöglich vor digitalen Angriffen zu schützen. Wenn Sie folgende Grundregeln beachten, können Sie sowohl im Büro als auch an Ihren mobilen Geräten sicher arbeiten.

Verschwiegenheit

Hochschulinterne und personenbezogene Informationen, insbesondere Zugangsdaten unterliegen der strikten Geheimhaltung. Verweigern Sie stets die Auskunft zu derlei Anfragen – vor allem dann, wenn eine Person Sie kontaktiert, die Sie nicht kennen.

Achtsamkeit

Achten Sie vor allem in der Öffentlichkeit auf Mithörende oder Mitlesende und behalten Sie Ihre Mobilgeräte im Auge, um den Zugriff durch Fremde/Dritte darauf zu verhindern.

Vorsicht

Neue technische Geräte, Datenträger oder Zusatzmodule sollten immer originalverpackt und von vertrauenswürdigen Quellen bezogen werden. Beispielsweise birgt selbst das kurzzeitige Anstecken eines ungeprüften USB-Sticks an einen PC die Gefahr eines Malware-Befalls. Setzen Sie jede Art von Technik nur nach Rücksprache mit dem IT-Service-Center (ISC) bzw. mit den zuständigen Administratoren der Bereiche und in Übereinstimmung mit unseren zentralen Sicherheitsrichtlinien ein.

Aufmerksamkeit

Datei-Anhänge und Verlinkungen zu vermeintlich seriösen Unternehmen (Post, Banken, Händler, Messeveranstalter u. v. a. m.) in sogenannten Phishing-E-Mails sind nach wie vor ein sehr häufig genutztes und übliches Eintrittstor für Angreifende. Vergewissern Sie sich (z.B. durch einen Anruf), ob die absendende Person Sie tatsächlich per E-Mail kontaktiert hat, bevor Sie Anhänge öffnen oder eine Verlinkung anklicken. Leiten Sie bitte jede einzelne Phishing-Mail ausschließlich als Anlage an *phishing@hs-anhalt.de* weiter oder verwenden den Meldeknopf in Ihrem Outlook-Programm.

Professionalität

Die Hochschule Anhalt verwendet für ihre dienstlichen PCs und Laptops ein modernes Anti-Malware-Programm, um diese vor den neuartigen Bedrohungen zu schützen. Profitieren Sie von zentralen, professionellen Lösungen, die Ihnen das IT-Service-Center über die zuständigen Bereichsadministratorinnen und -administratoren zum Schutz Ihrer dienstlichen Geräte zur Verfügung stellt.

Geheimhaltung

Passwörter sind wie ein persönlicher Schlüssel zu behandeln. Es sind geheime Informationen und diese müssen vertraulich behandelt werden. Benutzen Sie nach Möglichkeit einen Passwortmanager oder die im Download-Bereich der Webseite zur Informationssicherheit und zum Datenschutz zur Verfügung gestellte Passwortkarte, um sich Ihre Passwörter zu erstellen und zu merken.

Meldung

Wenn Ihnen etwas Verdächtiges auffällt, informieren Sie je nach Vorfall unverzüglich Ihren nächsten Vorgesetzten, Ihren zuständigen Kontakt im Bereich der IT-Administration bzw. die Informationssicherheits- oder Datenschutzbeauftragung der Hochschule. Denkbare Szenarien und die entsprechenden Zuständigkeiten erfahren Sie u. a. auch in der IT-Basisschulung oder auf unserer Website.
››› https://www.hs-anhalt.de/informationssicherheit/sicherheitsvorfall.html

Weiterbildung

Besuchen Sie die angebotenen Weiterbildungen und informieren Sie sich über die relevanten Themen der Informationssicherheit und des Datenschutzes. In offenen Diskussionsrunden haben Sie die Möglichkeit, Ihre Fragen zum Thema zu stellen und weiteres Wissen aufzubauen.

Sorgfalt

Richten Sie Gerätesperren ein und verwenden Sie für die interne Kommunikation außerhalb der Hochschule eine vom IT-Service-Center (ISC) zentral eingerichtete VPN-Verbindung. Kommunizieren Sie informationssicherheitskritische Informationen keinesfalls über ungeschützte Kanäle wie bspw. unsichere WLANs. Denken Sie auch an den Schutz Ihrer Privatsphäre bevor Sie etwas in den sozialen Medien posten. Wenn Ihre Daten in falsche Hände geraten oder Sie in sozialen Netzwerken zu viel von sich offenbaren, können Angreifende speziell auf Sie zugeschnittene Techniken entwickeln und Sie damit gezielt angreifen und manipulieren.

Entsorgen Sie schützenswerte Dokumente über geeignete Aktenvernichter und Datentonnen. Entsorgen Sie jegliche Datenträger ausschließlich über die Abgabe beim IT-Service-Center (ISC). Dort wird eine physische Zerstörung vorgenommen.

Lassen Sie sich notwendige und intern geprüfte Software ausschließlich von Ihrer/m zuständigen IT-Administrator/in installieren.

Vertrauen

Vertrauen Sie Ihrem Administratoren-Team und dem IT-Service-Center. In enger Zusammenarbeit mit Ihnen werden auch besondere Wünsche auf ihre Machbarkeit geprüft und realisiert.