



VOLLZEIT | 6 SEMESTER

BACHELOR

IT Security

Secure Software & Ethical Hacking | Secure Infrastructure & Networking | Operating Systems & Cloud Security | Security Management

IT Security

In einer vernetzten Welt stellen gezielte Cyberangriffe eine massive Bedrohung für Wirtschaft und öffentliches Leben dar. Es braucht daher Expert*innen, die Menschen und Organisationen dabei unterstützen, Systeme gegen digitale Gefahren abzusichern und Hackerangriffe abzuwehren.

Ihr Studium

Sie erhalten eine 360-Grad-Ausbildung in allen wesentlichen Schwerpunkten der IT Security:

Secure Infrastructure & Networking: Studierende erwerben Kenntnisse über Netzwerkprotokolle, Routing und Switching. Darauf aufbauend werden die wichtigsten Hardware-Komponenten und Protokollspezifika behandelt, um Netzwerke sicher planen und betreiben zu können.

Operating Systems & Cloud Security: Dieser Schwerpunkt vermittelt Wissen über verschiedene Betriebssysteme und deren Architekturen. Die Studierenden lernen, Windows- und Linux-Systeme zu administrieren sowie Sicherheitsrisiken zu erkennen und zu mitigieren.

Secure Software & Ethical Hacking: In diesem Schwerpunkt erwerben Studierende angewandte Programmier- und Datenbankkenntnisse in allen Phasen des Software Development Lifecycles. Der Sicherheitsaspekt steht dabei stets im Vordergrund.

Security Management: Der Schwerpunkt Sicherheitsmanagement beschäftigt sich mit Sicherheitsnormen und -standards für Unternehmen und umfasst Themen wie die Planung technischer, organisatorischer und menschlicher Abwehrmaßnahmen, das Risiko- und Notfallmanagement sowie rechtliche Grundlagen rund um Vertragsrecht und Datenschutz.

Ihre Jobaussichten

Wo sicherer IT-Betrieb gewährleistet oder sichere IT-Produkte entwickelt werden müssen, sind Sie als Absolvent*in des Bachelor-Studiengangs IT Security hoch gefragt. Je nach Interesse und Berufserfahrung können Sie auf unterschiedlichen Ebenen eines Unternehmens tätig sein. Unsere Absolvent*innen erwarten eine nahezu 100-prozentige Beschäftigungsquote.

Berufs- und Tätigkeitsfelder (Auswahl):

- Sicherheitsbeauftragte*r (Chief-Security-Officer / (Chief Information Security Officer)
- Security-Architekt*in
- Secure Software Developer
- IT Forensiker*in
- Security Cloud Specialist
- Security-Berater*in
- Netzwerk-/Betriebssystem-Administrator*in
- Datenschutzbeauftragte*r
- Auditor*in
- Informationssicherheitsmanager*in
- Disaster Recovery und Business Continuity Analyst oder Manager*in
- System, Application, Network / Web Penetration Tester*in
- Incident Responder



© Rauchecker Photography



Abschluss

Bachelor of Science
in Engineering (BSc)



Studiendauer

6/7 Semester



Studiengebühren

363,36 € pro Semester
+ ÖH-Beitrag



Bewerbung

bewerbung.fhstp.ac.at



Studienplätze/Jahr

35 Vollzeit
15 berufsbegleitend



Organisationsform

Vollzeit (6 Semester)
berufsbegleitend (7 Semester)

Das macht Ihr Studium einzigartig

Verknüpfung mit der Forschung

Durch die enge Verknüpfung mit dem Institut für IT Sicherheitsforschung stellen wir den Bezug zwischen Studium, aktuellen Themen sowie künftigen Entwicklungen der IT Security sicher.

Praxisnaher Unterricht & starke Vernetzung

Wesentlicher Teil der Ausbildung ist die Praxisnähe. In zahlreichen Projekten und Formaten wie der Krisenwoche bereiten Sie sich praktisch und theoretisch auf eine Vielzahl von Einsatzszenarien vor. In unserem Cyber Defense Center (CDC) erwerben Sie wichtige Kompetenzen rund um das Entdecken und Analysieren von schädlicher Aktivität in Netzwerken und Betriebssystemen. Zudem profitieren Studierende von einer engen Vernetzung mit Expert*innen aus der Praxis – sei es im Rahmen von Gastvorträgen oder bei Konferenzbesuchen.

Innovative Lehrmethoden

Innovatives Lernen wird bei uns großgeschrieben: Lehrveranstaltungen finden in Blockeinheiten statt, wodurch Sie sich zu jeder Zeit voll und ganz auf ein Thema konzentrieren können. In Inverted Classrooms oder beim Game

Based Learning trainieren Sie unterschiedliche Skills. Dabei stehen die praktische Anwendung und persönliche Betreuung immer im Zentrum.

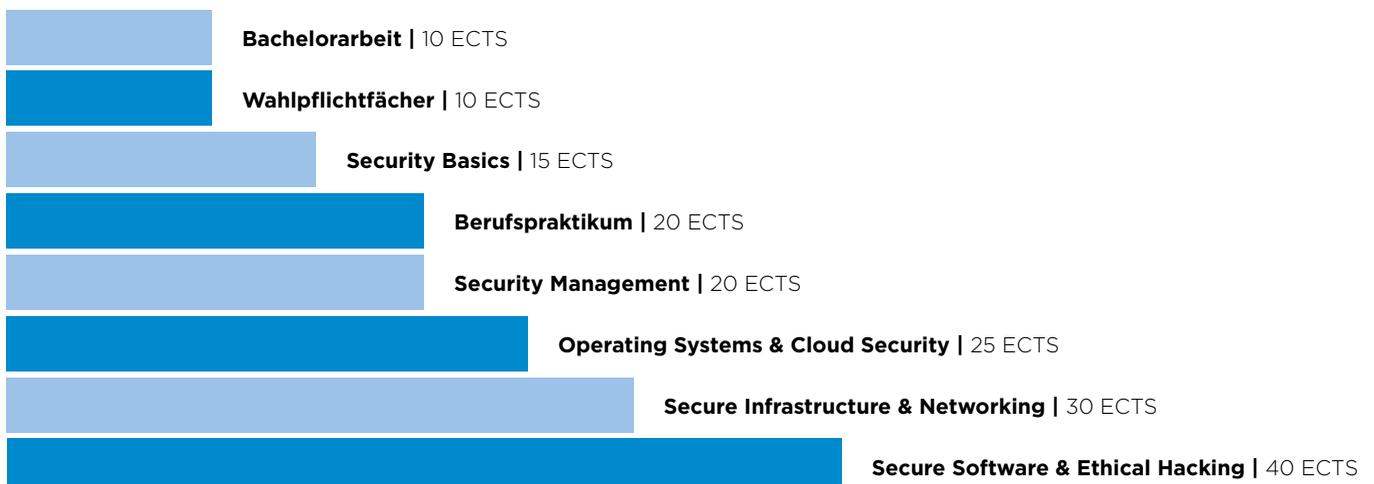
Moderne Infrastruktur

Für die Durchführung einer praxisorientierten Ausbildung stehen Ihnen 5 unabhängige Labore mit modernster PC- und Virtualisierungsinfrastruktur 24/7 zur Verfügung. Sie können die gesamte Infrastruktur rund um die Uhr nutzen – auch von Zuhause aus.

Studium und Beruf

Der Studiengang ist bestmöglich auf die Bedürfnisse von Berufstätigen abgestimmt – auch als Vollzeitstudium. Online-Lehrveranstaltungen machen etwa 20 Prozent des Studienplans aus, der Unterricht findet von Montag bis Donnerstag statt. Beim berufsbegleitendem Studium findet der Unterricht Donnerstagabend online sowie Freitagnachmittag und Samstag in Präsenz statt. Die verpflichtenden Berufspraktika (12 Wochen) können über die gesamte Studiendauer verteilt absolviert werden. Studierenden, die bereits facheinschlägig arbeiten, wird das Praktikum angerechnet.

Gewichtung der Studieninhalte



Studienplan (berufsbegleitend)

1. Studienjahr

1. Semester	ECTS
Team Training & Conversation	5
Mathematics for Security Experts	5
Networks & Distributed Systems	5
Windows Administration	5
OS Fundamentals & Linux Security	5

2. Semester	ECTS
Building Computer Networks	5
Network Protocols	5
Cryptography	5
Coding Basics	5

Das verpflichtende Berufspraktikum im Umfang von 20 ECTS kann über die gesamte Studiendauer verteilt absolviert werden.

2. Studienjahr

3. Semester	ECTS
Network Security	5
Secure Coding & Database Fundamentals	5
Advanced Coding & Database Technologies	5
Security Management 1 - Basics & Systems	5
Security Management 2 - Code of Practice	5
Internship	4

4. Semester	ECTS
CDC Operations	5
Secure Software Engineering	5
Web & Application Security	5
Digital Forensics	5
Security Management 3 - Risk & Business Continuity	5
Internship	4

3. & 4. Studienjahr

5. Semester	ECTS
Mobile Systems & Authentication	5
Essential Hacking Tools & Penetration Testing	5
Research Practices & Scientific Writing	5
Operating Systems Hardening	5
Internship	4

6. Semester	ECTS
Cloud Computing & Cloud Security	5
Building Secure Architecture	5
Elective 1	5
Elective 2	5
Internship	4
Security Management 4 - Awareness, Outsourcing & Law	5

7. Semester	ECTS
Business Continuity Exercise	5
Bachelor Thesis	10
Project Management	5
Internship	4

Studienplan (Vollzeit)

1. Semester	ECTS
Team Training & Conversation	5
Mathematics for Security Experts	5
Networks & Distributed Systems	5
Coding Basics	5
Windows Administration	5
OS Fundamentals & Linux Security	5

2. Semester	ECTS
Building Computer Networks	5
Network Protocols	5
Cryptography	5
Secure Coding & Database Fundamentals	5
Security Management 1 - Basics & Systems	5
Security Management 2 - Code of Practice	5

3. Semester	ECTS
Network Security	5
CDC Operations	5
Secure Software Engineering	5
Web & Application Security	5
Advanced Coding & Database Technologies	5
Security Management 3 - Risk & Business Continuity	5

4. Semester	ECTS
Mobile Systems & Authentication	5
Essential Hacking Tools & Penetration Testing	5
Digital Forensics	5
Operating Systems Hardening	5
Cloud Computing & Cloud Security	5
Security Management 4 - Awareness, Outsourcing & Law	5

5. Semester	ECTS
Internship	20
Project Management	5
Research Practices & Scientific Writing	5

6. Semester	ECTS
Business Continuity Exercise	5
Building Secure Architecture	5
Elective 1	5
Elective 2	5
Bachelor Thesis	10

Alle Details
und Infos
zur Aufnahme



Blieben Sie auf Social Media up-to-date!

📷 Instagram Informatik & Security: [instagram.com/fhstp_informatik_security](https://www.instagram.com/fhstp_informatik_security)

📷 Instagram: [instagram.com/fhstp](https://www.instagram.com/fhstp)

🎵 TikTok: [tiktok.com/@fhstp](https://www.tiktok.com/@fhstp)

🌐 LinkedIn: [linkedin.com/school/fhstp](https://www.linkedin.com/school/fhstp)



© Raucherker Photography

Information & Kontakt

Campus und Study Center (CSC) | T: +43 2742 313 228-333 | E: csc@fhstp.ac.at | I: fhstp.ac.at

Diversität am Campus St. Pölten

Inklusion, Geschlechtergerechtigkeit und Vielfalt sind uns wichtig. Unser Campus ist barrierefrei zugänglich. Bitte nehmen Sie rechtzeitig mit uns Kontakt auf, damit wir Ihre Bedürfnisse berücksichtigen können.

09/2024