fhwn.ac.at/lccri
Lehrgang (LG) **| akademisch geprüfte*r Cybercrime-Expert*in (a.E.) | Berufsbegleitend**
2 Semester, 60 ECTS

Campus 1, Wiener Neustadt

FACHHOCHSCHULE
WIENER NEUSTADT
University of Applied Sciences – Austria

Cyber Crime Investigation LG

Mit präzisem Fachwissen Cyberkriminalität erkennen und verstehen, digitale Spuren verfolgen und strafrechtliche Sachverhalte analysieren.

Ausgangspunkt des Lehrgangs ist ein integrativer Blick auf Bedrohungen, Abwehr und Ermittlung. Behandelt werden Architektur und Schutz von Netzwerken und Informationen, Datenanalyse und Kryptografie, die Auswertung mobiler und stationärer Spuren sowie die juristische Einordnung. Auch gesellschaftliche und ethische Dimensionen werden berücksichtigt. Ziel ist es, fundierte Entscheidungen entlang des gesamten Sicherheitsprozesses – von der Bewertung bis zur Dokumentation – treffen zu können.

HIGHLIGHTS

- **Interaktive Simulationen und reale Fallanalysen**
- **Analyse zentraler Kriminalitätsaspekte: Identitätsdiebstahl, Datenmissbrauch, Desinformation**
- **Internationale Zusammenarbeit & Verfahren im grenzüberschreitenden Kontext**

Die **Capture-the-Flag-Simulation** bietet eine geschützte Trainingsumgebung: Teams analysieren reale Angriffsbilder, erkennen Schwachstellen strukturiert und leiten Gegenmaßnahmen ab. So wird das Zusammenspiel von Technik, Forensik und Recht unter Zeitdruck trainiert – messbar und risikofrei.

KEYFACTS

- **Deutsch** (teilweise Englisch)
- **Studienstart Februar**
- **Präsenz** im Zweiwochenrhythmus (Do/Fr 8–22 Uhr, Sa 8–18 Uhr); einzelne Einheiten online
- **Kurskosten** unter **fhwn.ac.at/lccri**
- **Kontakt: sicherheit@fhwn.ac.at**

STUDIENINHALTE & STRUKTUR

Sieben Module decken Themen von technischer Infrastruktur über digitale Beweismittel bis hin zu regulatorischen und ethischen Fragen ab. Den Abschluss bildet ein eigenständiges Projekt, das vor einer Prüfungskommission präsentiert und verteidigt wird.

- **Einbindung aktueller Standards (z. B. ISO-27001, NIS2, EU AI Act, Cyber Resilience Act)**
- **Module: Orientierung, Recht, Technik, Cyber-Bedrohung, Cyber-Abwehr, Cyber-Ermittlung, Cyber-Prävention**
- **Bedrohungsmodelle, Täterprofile & Anonymisierungsnetzwerke im Dark-Web**

LEHRGANG IM DETAIL:

QR-Code scannen und alle Details zum Lehrgang entdecken.
Videos, Projekte, Podcasts und vieles mehr!

Check us out @fhwn

LEHRINHALTE & CURRICULUM

1. Semester	ECTS 30
Einführung Cybercrime,Cybersecurity, Cyberdefense	2,5
Wissenschaftliches Arbeiten, Reporting	2,5
Strafrecht im Cyberspace	2,5
Zivilrecht im Cyberspace	2,5
Grundlagen der technischen Kommunikation	1,5
Netzwerk, Hardware und Datenträger	2
Systementwicklung	1,5
Data Science	2,5
Kryptografie	2,5
Computerkriminalität	5
Angriff auf IT-Systeme	2,5
Desinformation und Radikalisierung	2,5

2. Semester	ECTS 30
Netzwerksicherheit	5
Informationssicherheit	5
IT-Forensik	2,5
Mobile Forensik	2,5
Sicherung digitaler Beweismittel	2,5
Erscheinungslehre	2,5
Technische Ermittlungen	2,5
Polizeiliche und justizielle Kooperation	2,5
Lessons from the bad side of business	1,5
Abschlussprojekt inkl. Defensio	3,5

Studienplan vorbehaltlich inhaltlicher Änderungen. Aktueller Studienplan unter **fhwn.ac.at/lccri**

KOOPERATIONEN

Bundesministerium Inneres

Bundesministerium Inneres
Sicherheitsakademie

Bundesministerium Inneres
Bundeskriminalamt

POLIZEI

MODULAUFBAU

Ausgehend von Recht und Technik als Kernmodule bauen die weiteren Cyber-Module aufeinander auf. Nachfolgend eine Übersicht mit ausgewählten Lehrveranstaltungen:

Orientierung

- Vermittelt Grundlagen digitaler Sicherheit & führt in wissenschaftliches Arbeiten ein.
- **Einführung Cybercrime, Cybersecurity, Cyberdefense (1. Semester):** Überblick über digitale Sicherheit, Bedrohungsformen und grundlegende Abwehrstrategien.

Core Recht

- Behandelt rechtliche Aspekte der digitalen Welt & aktuelle europäische Regelwerke.
- **Strafrecht im Cyberspace (1. Semester):** Anwendung des Strafrechts auf Hacking, Datenmissbrauch und internationale Ermittlungen.

Core Technik

- Technische Grundlagen zu Netzwerken, Datenanalyse und Verschlüsselung.
- **Data Science (1. Semester):** Arbeiten mit Datenbanken, Analyseverfahren und Python – Grundlage datengetriebener Entscheidungen.

Cyber Bedrohung

- Untersucht Angriffsformen, Täterprofile und digitale Manipulationen.
- **Computerkriminalität (1. Semester):** Täterprofile, Dark-Web-Strukturen und reale Fallanalysen zur digitalen Kriminalität.

Cyber Abwehr

- Vermittelt Strategien und Maßnahmen zum Schutz von IT-Systemen.
- **Informationssicherheit (2. Semester):** Cloud-Security, Schwachstellenmanagement und Penetrationstests in modernen IT-Umgebungen.

Cyber Ermittlung

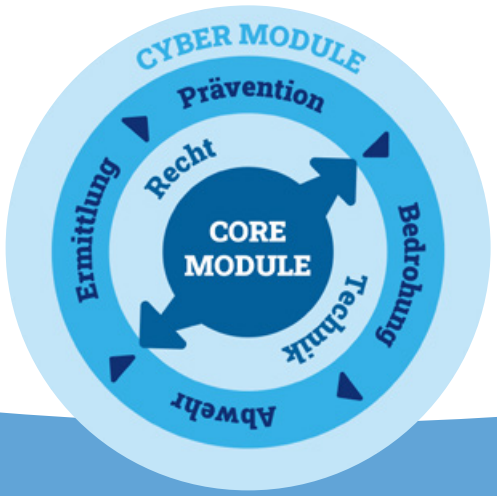
- Fokus auf digitale Spurensicherung und forensische Methoden.
- **Mobile Forensik (2. Semester):** Analyse und Spurensicherung auf Smartphones und Tablets unter realen Bedingungen.

Cyber Prävention

- Praxisnahe Simulationen, Risikomanagement und Abschlussprojekt.
- **Lessons from the bad side of business (2. Semester):** Simulation realer Cyberangriffe und Krisenentscheidungen in interaktiven Planspielen.

ZIELGRUPPE

Der Lehrgang ist speziell auf berufstätige Personen mit Vorbildung oder Berufserfahrung im Sicherheits-, IT- oder Rechtsbereich zugeschnitten. Eine technische Grundkenntnis wird vorausgesetzt – jedoch kein spezifischer IT-Abschluss.



BEWERBUNG & AUFNAHME

1. **Bewerben unter fhwn.ac.at/bewerbung**
   Ein abgeschlossenes österreichisches oder gleichwertiges ausländisches Hochschulstudium (mind. auf Bachelorniveau mit mind. 180 ECTS), oder allgemeine Universitätsreife & mind. zwei Jahre einschlägige Berufserfahrung (Aus- & Weiterbildungszeiten können eingerechnet werden), oder mind. vier Jahre einschlägige Berufserfahrung
2. **Einladung zum Aufnahmetag – die Aufnahmegespräche finden im Dezember statt.**
3. **Schriftliche Benachrichtigung über das Ergebnis.**

FH Wiener Neustadt GmbH
Campus 1 Wiener Neustadt
Johannes Gutenberg-Straße 3,
2700 Wiener Neustadt
+43 5 04211
office@fhwn.ac.at | fhwn.ac.at

Stand: 10/2025, Foto-Credits: FH Wiener Neustadt, stock.adobe.com