Master of Cybersecurity

swinburne.edu.au/international

The Master of Cybersecurity is designed for students who wish to deepen their computer science and cyber security knowledge by focussing on identifying, diagnosing and fixing flaws in software systems such as web applications, internet-based services and desktop applications.

The course focuses on practical aspects of cybersecurity including system security, penetration testing, incident response, security management, reverse engineering and ethical hacking.

The course has been developed in conjunction with industry experts and designed around a project-based learning methodology to better prepare students for current best practice and process within the industry.

Course snapshot

Duration	Two years full-time
Campus	Hawthorn (Melbourne)
Fees	A$34,000*
Intakes	March, August

*Fees displayed are relevant to 2019 and are subject to annual review. Fees are based on a student's study load in each semester. Please see website for more.

Entry requirements

- A recognised bachelor degree in STEM (Science, Technology, Engineering or Mathematics_ or
- A non-STEM bachelor degree plus 3 years industry experience in web development, cybersecurity, software development or related fields
- English language proficiency (please see website for details)

Scholarship opportunities

Scholarships of up to 25 per cent off tuition fees are available for selected students who apply for and begin this two-year master by coursework program. For more on scholarships, visit **swinburne.edu.au/international/scholarships**

Why Swinburne?

A world-ranked university in Melbourne, Australia, Swinburne is focused on creating careers. Upon graduation, our students are career-ready professionals who regularly find employment with the world's best companies, including PricewaterhouseCoopers, IBM, Siemens, Mercedes-Benz and more.

Swinburne is proud to be recognised as one of the world's top universities under 50 years, ranked number 45 in the 2019 QS Top 50 Under 50.

Situated in Hawthorn, just ten minutes by train from Melbourne's city centre, Swinburne boasts shops, cafes and a train station right on its doorstep. With high-quality teaching and research, state-of-the-art facilities, student accommodation options and a range of support services, Swinburne is the ideal choice for students.

Industry connections

For over 50 years, Swinburne University of Technology has been partnering with leading organisations to offer students practical learning and authentic workplace experiences. Our postgraduate programs are co-designed with industry, and many of our students undertake industry-linked projects or projects with their own employers as part of their studies.

We are really proud of this course. At Swinburne we pride ourselves on producing employment ready graduates with a great depth of understanding. In this course we particularly emphasises the hands-on, practical aspects of computer security by giving students experience in hacking, programming, patching and bug fixing. We give students project work so that they can pursue a deep understanding in areas of particular interest to them. We have great facilities, enthusiastic capable teachers and strong links with industry.

We believe this course will produce graduates with the depth and breadth to build a successful career in cybersecurity.

Associate Professor Philip Branch
Studying Master of Information Technology

Course overview

You must complete units of study as follows:

- 6 core academic units (as below)
- 3 core project-based learning units (as below)
- 1 or 2 elective units

Core Cybersecurity units

- Creating Web Applications
- Introduction to Network Programming
- Operating System Management
- Networks and Switching
- Cyber Ethics
- Internet Security
- Operating System Cybersecurity
- Advanced Cybersecurity Programming

Core Cybersecurity units

- System Security Project
- Glass Box Project
- Reverse Engineering Project

Semester Study Themes

You will undertake your studies grouped under three distinct themes that focus on the processes and techniques used by cybersecurity professionals used in the industry. Following the first semester of studies to establish your theoretical knowledge, each semester is designed around an industry project related to corresponding theme with support units to properly introduce relevant technical content. Elective units are available in the final two semesters to allow you to customise your study experience.

System Security

You will undertake a guided System Security project in your second semester of this course where you will be exposed to current industry practices and techniques in guided projects involving team and individual challenges. The Supporting units will introduce you to the terminologies and tools associated with cybersecurity, along with building a comprehensive framework to understand the ethical issues associated with deploying cybersecurity solutions.

Units of study

- Cyber Ethics
- Internet Security
- System Security Project

Glass Box Security

You will undertake an industry-sourced project with an unknown solution requiring you to become a pro-active, self-managed learner. The Glass Box theme revolves around Cybersecurity problems where students will be able to observe the internal workings of existing systems but not be able to directly modify them. Solutions in this space revolve around deploying external "shims" to protect these existing systems. You will learn techniques for automating attacks and security testing. The support unit will introduce the internal workings of operating systems and common attack vectors.

Units of study

- Operating System Cybersecurity
- Glass Box Project

Reverse Engineering Security

You will undertake an industry-sourced project with an unknown solution requiring you to become a pro-active, self-managed learner. The Reverse Engineering theme revolves around Cybersecurity problems where students will be expected to explore the internals of existing systems to determine how they function, and then to deploy modifications to third party software to resolve any discovered issues. The support unit will cover assembly language programming and e-Forensic techniques to analyse and modify existing applications in real time.

Units of study

- Advanced Cybersecurity Programming
- Reverse Engineering Project

Elective Units

- Research Paper
- Minor Thesis
- Secure Networks
- Big Database
- Internship Project

Career outcomes

The Master of Cybersecurity is a unique course that offers an industry oriented technical course which prepares graduates for a career in cybersecurity testing, incident response, auditing and malware analysis.

Unlike other cybersecurity Masters courses, this course is designed from the ground up to be specific to the needs of aspiring penetration testers, application developers and web programmers. The course is informed by the work of the Open Web Application Security Project (OWASP) and includes contributions by industry leaders such as Kaspresky, Microsoft, CyberGum and CISCO.

How to apply

Visit our website for step-by-step application instructions:
www.swinburne.edu.au/international/apply/

More information

+61 3 9214 8444 (outside Australia)
1300 275 794 (within Australia)
international@swinburne.edu.au
swinburne.edu.au/it

CRICOS 00111D RTO 3059