

STEM & Cyber Safety Programs for Australian Schools

Program brochure · Years 3 to 12 · Delivered by working security engineers

Fast Emu is a Melbourne-based managed cyber security provider. Our education team brings the same engineers who defend Australian businesses into classrooms, so students learn digital safety and security thinking from people who do the work every day. Every program is curriculum-aligned, teacher-friendly, and can be delivered in class, online, or as a holiday program.

At a glance

Program	Year levels	Duration	Format
Cyber Safety Explorers	Years 3–6	4 sessions × 45 min	In class, teacher present, mostly unplugged
Code & Defend	Years 7–9	6 weeks × 60 min	School laptops, Python 3 in a browser sandbox
Future Cyber Careers	Years 10–12	2 sessions × 90 min	In class or online, careers-team friendly
Passkeys & Privacy	Years 6–12	Single 60 min workshop	Whole year level, hall or theatre friendly
Holiday Cyber Camp	Years 7–10	2 days × 5 hrs	Melbourne venue, small groups of 16
Teacher & Parent Briefings	Staff and families	60 min evening session	On site or webinar, recording provided

Why schools book us

- Curriculum-aligned to the Australian Curriculum: Digital Technologies and related capabilities.
- Facilitators are practising security engineers, with Working with Children Checks.
- Unplugged options for primary — no device rollout or IT setup required.
- Teacher notes, slides and take-home family activities included.
- Reporting pack after delivery: participation, assessment results and observations.

YEARS 3-6

Cyber Safety Explorers

4 sessions × 45 min · In class, teacher present, mostly unplugged

A story-led introduction to staying safe online, built around characters students recognise from their own group chats and games.

Learning outcomes

- Create and remember a strong passphrase without writing it down
- Identify three signals that a message is a scam
- Describe what personal information should never be shared online
- Name two trusted adults to tell when something feels wrong

Session plan

Session 1 — Secrets and passphrases

Students crack weak passwords by hand, then build a four-word passphrase and test how long it would take to guess. Unplugged card activity, no devices required.

Session 2 — Spotting the scam

A gallery walk of real (anonymised) scam texts and emails seen in Australia. Students hunt for red flags and build a class 'scam detector' poster.

Session 3 — What stays private

Sorting game across public / classroom / private information, including screenshots, locations and school uniforms in photos.

Session 4 — Getting help fast

Role-play of what to do when an account is taken over, plus how to report in-game harassment. Students write their own help plan to take home.

Curriculum alignment

- Digital Technologies: Privacy and security of data (AC9TDI4P09)
- Health & PE: Safety and help-seeking
- General capability: Digital Literacy — Practising digital safety and wellbeing

Assessment

Short 10-question quiz plus a take-home family passphrase challenge.

YEARS 7-9

Code & Defend

6 weeks × 60 min · School laptops, Python 3 in a browser sandbox

A term module that blends Python fundamentals with defensive thinking — students write code, then attack and protect it.

Learning outcomes

- Write Python functions using variables, loops and conditionals
- Encrypt and decrypt a message with a Caesar and a substitution cipher
- Explain how password hashing and salting protect stored credentials
- Describe how a login flow can be attacked and how MFA breaks the attack

Session plan

Week 1 — Your first defensive script

Python setup, variables and input validation. Students build a passphrase strength checker and test it on each other's ideas.

Week 2 — Ciphers by hand, then in code

Caesar cipher on paper, then implemented in 15 lines of Python. Introduces loops, string indexing and modular arithmetic.

Week 3 — Hashing and why passwords aren't stored

Students hash their passphrases, see identical inputs produce identical hashes, and discover why salting matters using a leaked-password lookup demo.

Week 4 — How logins really work

Walkthrough of a request/response cycle with a simple mock login, brute-force demo against a weak account, then adding rate limiting and MFA.

Week 5 — Build the blue team playbook

Teams triage a simulated incident timeline (odd logins, a suspicious inbox rule) and write a short containment plan in plain English.

Week 6 — Friendly capture the flag

Six beginner challenges across ciphers, log reading and web basics, run in a closed sandbox with a leaderboard and a team debrief.

Curriculum alignment

- Digital Technologies: Implementing (AC9TDI8P05, AC9TDI10P06)
- Digital Technologies: Data representation and encryption
- Mathematics: Patterns, number systems and probability

Assessment

Portfolio of Python scripts, the blue-team playbook, and a CTF score with facilitator feedback.

YEARS 10-12

Future Cyber Careers

2 sessions × 90 min · In class or online, careers-team friendly

Pathways and practice: what security work actually looks like day to day, and the subjects and steps that lead there.

Learning outcomes

- Describe four distinct security roles and the skills each needs
- Read a security alert and decide whether it warrants escalation
- Map at least one realistic pathway from Year 12 to a first security role
- Identify Australian entry routes: TAFE, university, traineeships and certifications

Session plan

Session 1 — A day in the SOC

Live look at an anonymised operations dashboard. Students triage three alerts in pairs, then compare their calls with what our analysts actually did.

Session 2 — Pathways and portfolios

Roles, salaries and study routes across Australia, plus how to build a credible portfolio at school: home labs, CTF platforms, and safe practice rules.

Curriculum alignment

- Work Studies: Career development and pathways
- Digital Technologies: Investigating and defining, evaluating
- VCE/HSC subject-selection guidance for IT and mathematics

Assessment

Each student leaves with a one-page personal pathway plan.

YEARS 6-12

Passkeys & Privacy

Single 60 min workshop · Whole year level, hall or theatre friendly

A high-energy single session on multi-factor authentication, passkeys and the size of a personal data footprint.

Learning outcomes

- Explain the difference between a password, an SMS code and a passkey
- Set up a passkey or authenticator app on a personal device
- Audit the permissions granted to one app they already use

Session plan

Part 1 — Breaking a password live

Facilitator-led demonstration of credential stuffing against a dummy account, then the same attack failing against a passkey.

Part 2 — Lock it down

Guided device walkthrough: enable MFA, create a passkey, and review app permissions and location sharing.

Curriculum alignment

- Digital Technologies: Privacy, security and data protection
- General capability: Digital Literacy — Managing online identity

Assessment

Exit ticket: one control each student enabled during the session.

YEARS 7-10

Holiday Cyber Camp

2 days × 5 hrs · Melbourne venue, small groups of 16

Students build, break and defend a small network in a safe sandbox, finishing with a demo to parents.

Learning outcomes

- Build a small virtual network with a server, client and firewall
- Run a supervised attack against their own environment and detect it in the logs
- Present findings and fixes to a non-technical audience

Session plan

Day 1 — Build it

Networking basics, IP addressing, spinning up virtual machines, and standing up a simple web service behind a firewall.

Day 2 — Break it, then defend it

Supervised attacks on their own build, log analysis to find the evidence, hardening changes, and a short showcase to families.

Curriculum alignment

- Digital Technologies: Networks and systems
- Science inquiry skills: Planning, conducting and evaluating

Assessment

Team showcase plus a written before/after hardening summary.

STAFF AND FAMILIES

Teacher & Parent Briefings

60 min evening session · On site or webinar, recording provided

Free briefings so the conversation continues after we leave, with classroom-ready resources for staff.

Learning outcomes

- Recognise the scams and grooming patterns currently targeting students
- Know the escalation path when a student account is compromised
- Use the supplied lesson starters in existing subject time

Session plan**Briefing — What we're seeing in Australian schools**

Current threat patterns, real anonymised examples, family device agreements, and a Q&A; with the facilitators.

Curriculum alignment

- School child-safe and digital-wellbeing policy support
- Professional learning: integrating digital safety across subjects

Assessment

Not assessed — attendees receive a resource pack and slide deck.

Booking a program

How it works

1. Tell us the year levels, class sizes and dates you have in mind.
2. We send a short delivery plan, teacher notes and a quote — usually within two business days.
3. We confirm facilitators, Working with Children Check details and any IT requirements with your school.
4. Delivery, followed by a reporting pack and an optional teacher or parent briefing.

Contact

Email: hello@fastemu.tech

Web: fastemu.tech/stem

Book a consultation: fastemu.tech/consultation

Programs, session counts and durations can be tailored to your timetable. This brochure is indicative and does not form part of a contract.