CAREERS WITH STEM™

CYBER SECURITY

DOUBLE ISSUE
FLIP OVER FOR TECHNOLOGY

Meet the people keeping your money safe from hackers
p5

We bust the myths about real-life cyber careers
p10

Challenge your cyber skills while still in school
p8

DIGITAL FORENSICS

CAREERSwithSTEM.COM

SUPPORTED BY

Commonwealth Bank

ESSENTIAL SKILLS **+** MYTH BUSTING **+** COMPETITIONS **+** PATHWAYS

Schools Cyber Security Challenges

The **Schools Cyber Security Challenges** are designed to equip students with cutting edge cyber security skills, providing teachers with resources to support the teaching of cyber security concepts, and inform students of career opportunities in the field.

The Challenges are classroom ready, and aligned with both the **Australian Curriculum: Digital Technologies** and the **ICT Capability**.

An introduction to information security

Data encryption and transmission

Wired and wireless network security

Web application security

FREE interactive classroom activities aligned to the Australian Curriculum: Digital Technologies

Visit: **aca.edu.au/cyber**

Developed by the ACA in partnership with:

FIND YOUR DREAM JOB IN CYBER SECURITY

Cyber security is a broad, diverse – and growing! – discipline, with job opportunities to match your skills and interests

SHUTTERSTOCK, LAUREN TROMPP

When you think of cyber security, what – or who – comes to mind? Is it hackers in hoodies, bright screens in dark rooms? Or is it someone like me?

I graduated from the University of Western Australia with a Bachelor of Arts. After working in the public service for seven years, I was approached to join their cyber security team, and now my career in cyber security has spanned more than a decade. In my current role at the Commonwealth Bank of Australia, I'm focused on delivering training and education initiatives to improve cyber security behaviour.

Cyber security is for people who want to make a difference in their career, who are creative and like to solve problems collaboratively. In addition to ace coders and hackers, we need talent from a broad range of disciplines like data science, research, business, marketing, project management, communication and psychology (just to name a few!).

In this magazine, you'll read about men and women from different backgrounds, people who are obsessed with tech, and people who've never coded in their life –

SAMANTHA WOOD
CYBER OUTREACH MANAGER

what they all have in common is that they're passionate about keeping Australians and Australian businesses safe online.

Start asking yourself if you want to be part of one of the fastest growing and crucial sectors worldwide? An industry that's crying out for people who are curious, adaptable and have good communication skills.

If that sounds like you, then you'll find a career where you can make a real difference in a fast-paced, exciting field filled with passionate people, wonderful mentors and continuous learning opportunities.

Samantha Wood
Cyber Outreach Manager, Commonwealth Bank of Australia

CYBER SECURITY BY NUMBERS

STATS:

$426 BILLION CONTRIBUTION OF DIGITAL ACTIVITY TO THE AUSTRALIAN ECONOMY

300% GROWTH IN THE AUSTRALIAN CYBER SECURITY SECTOR PREDICTED BY 2026

17,000 NUMBER OF ADDITIONAL CYBER SECURITY WORKERS NEEDED IN AUSTRALIA BY 2026

163,000 NUMBER OF JOBS THAT COULD BE DISPLACED BY FOUR WEEKS OF DISRUPTION TO DIGITAL ACTIVITY AS A RESULT OF A CYBER ATTACK

$5 BILLION COST TO THE ECONOMY FROM JUST ONE WEEK OF DISRUPTION TO DIGITAL ACTIVITY AS A RESULT OF A CYBER ATTACK

Source: AustCyber

Which cyber security role suits you?

Want to know which box to tick when sussing out cyber roles? Quiz yourself!

1. Your phone starts acting weird. Do you:
A Check out hashtags for news on trending attacks
B Update your software and change your passwords, pronto
C Throw your phone away and get a new untraceable, non-GPS handset

2. You're taking part in a cyber security challenge. What's your role?
A Leader. Obvs
B Coding and testing
C Watching the other teams closely for any signs of suspicious behaviour

3. You're given a tricky puzzle to solve. What's your starting point?
A Research similar puzzles online and see if you can spot any trends
B Build software that can reverse engineer the problem
C Check out the credentials of the person that sent you the puzzle

ANSWERS:

MOSTLY As: Analyst
You're ace at getting the insights and intel together to think big picture, understanding the problem as well as acting on it. Project management and communication skills are key. Head to p5 to get more dirt.

MOSTLY Bs: Engineer
Security engineers create new security software. You're enterprising, creative and a team player and can work with a wide range of people to understand and troubleshoot issues that arise. See p14 for inspo.

MOSTLY Cs: Crime fighter
Digital forensic specialists are frontline crime fighters, running counter-hacking operations. You need to be a critical thinker and investigator, with an excellent understanding of cyber security practice. Get started on p10.

CYBER SECURITY

ARTS STUDENTS WANTED!

EXCELLENT AT ENGLISH? LOVE DELVING INTO HISTORY? HAVE A PASSION FOR MUSIC? YOU MIGHT BE SURPRISED AT THE SKILLS THAT ARE RELEVANT TO CYBER SECURITY CAREERS

Communication, analytical thinking, and creativity are all essential skills emphasised in humanities subjects. So, it's no surprise that areas that have traditionally been seen as 'arts' are in high demand in cyber security careers.

Australia will require an additional 17,000 cyber security professionals by 2026 – and people of diverse genders, backgrounds, cultures and regions are highly sought after. Professor Ryan Ko is chair and director of UQ Cyber Security at the University of Queensland and runs a program that aims to attract grads from all degree areas. "We take people from any background – you can have a degree in language, or music and still be accepted into cyber security," he says.

"Many of the cyber security challenges the government and industry face are highly complex. You need to decide whether threats come from activism, geopolitical activity or criminal activity," says Ryan. "If you understand cyber security you can work everywhere from preventing crime to policy."

Diverse thinkers

Rachael Williams is the enterprise business manager for technology company HP, which supports five scholarships for women to study the Masters of Cyber Security at the University of Queensland.

"One of the critical things you want students to be able to do is think critically and collaborate effectively," she says.

"In the corporate world you're not making decisions by yourself – you need to present a business case and work collectively to make a project happen, and to get people to follow you. Our passion is to get girls engaged as early as possible and understand what STEM learning is, how it connects to a career and that you don't need to be great at maths!"

Head higher

Alisha Hummel is a cyber security consultant for KPMG and mentor for the Victoria Indigenous Engineering Winter School. She moved into a degree in cyber security after initially thinking of going into law.

Alisha says skills such as communication, management and being adaptable and flexible are important to her job helping government and financial industries safeguard against cybercrime. "I love a challenge!" she says. "It does sound cliche to say, but not every day is the same." – *Heather Catchpole*

GET THESE SKILLS:

✔ Critical analysis
✔ Problem-solving
✔ Communication
✔ Teamwork
✔ Creativity
✔ Leadership
✔ Strategic thinking

ALISHA HUMMEL
CYBER SECURITY CONSULTANT

BACHELOR OF CRIMINOLOGY/BACHELOR OF IT (IT SECURITY), DEAKIN UNIVERSITY >>> BUSINESS INTELLIGENCE ANALYST, ADAIRS RETAIL GROUP >>> SENIOR CYBER SECURITY CONSULTANT, KPMG

SHANIS LOVIN
DIGITAL FORENSICS

DIGITAL DETECTIVE

SHANIS LOVIN TRACES THE FOOTPRINTS LEFT BY CYBER CRIMINALS – BUT THERE'S MORE TO HER JOB THAN CODING AND TECH

Everything we do online leaves a digital footprint. Shanis is one of the Commonwealth Bank of Australia's (CBA) 2020 Enterprise Services graduates and a member of the digital forensics team. Her job is to make sure data is recorded as evidence for trials or investigations. "None of this evidence can be messed with, just like in real life," she says.

Shanis started out with CBA in the summer holiday internship program while studying for a Bachelor of Information Technology at Macquarie Uni. She gained some great experience in software development and operations (DevOps) and stayed on as a part-time intern until she moved on to cyber security after finishing her degree.

"In the grad program you can do anything," she says, adding that the rotations between different teams helped her choose her current career path.

NOT JUST TECH SKILLS

Shanis says one of the big surprises when starting out in cyber security was the number of roles available and the range of skills needed.

"A lot of the roles aren't technical," she says. For example, the cyber-strategy team uses problem-solving skills to keep the bank secure and communicates these solutions to other teams. The cyber outreach team shares information about cyber security with the general public and teach people how to stay safe online, and interpersonal skills are important across all cyber roles.

"Communicating with people is important, as is your knowledge and understanding of how attacks happen," says Shanis. She adds people management, collaboration, critical thinking and innovation to the list of useful skills.

"You need to think outside the box. Attackers are not going to take the easy route."

GIVE IT A SHOT

During her degree and internship, Shanis tried everything from video-game coding and computer graphics to web development and cryptography. Cyber security may sound mysterious or even intimidating, but Shanis says it's a fun experience with a supportive team. "It's worth giving it a shot. You'll never know unless you try!" – *Nadine Cranenburgh*

GRADUATE PROGRAM. CBA

ENTERPRISE SERVICES INTERN. CBA

WEB TEAM INTERN. MACQUARIE UNIVERSITY

BACHELOR OF INFORMATION TECHNOLOGY (SOFTWARE TECHNOLOGY). MACQUARIE UNIVERSITY

> YOU NEED TO THINK OUTSIDE THE BOX. ATTACKERS ARE NOT GOING TO TAKE THE EASY ROUTE"

LAUREN TROMPP

CYBER SECURITY

ANDRZEJ GRZESLAK
PEN TESTER

A DAY IN THE LIFE OF A PEN TESTER

Discover what work looks like for an 'ethical hacker' at Australia's biggest bank

COVID-19 restrictions may have put a dent in the after-work foosball competition, but Commonwealth Bank of Australia (CBA) penetration tester (pen tester), Andrzej Grzeslak still loves the varied nature of his role and learning something new every day.

Andrzej's original goal was to become a software engineer, but a practical pen-testing subject at uni changed his mind. He really enjoyed the process of understanding how a piece of hardware or software worked, then pulling it apart to try and find its weaknesses.

"It's funny that I get paid to try and break things!" he says.

Andrzej came top of his class in the pen testing subject, which was sponsored by CBA. After trying out a software engineering role during the last year of his degree, Andrzej applied for the Enterprise Services grad program at CBA. He is now a pen tester in the cyber security team, with the important job of seeking out and reporting security flaws in hardware and software.

Andrzej says his role is very varied – one day he might be testing basic web apps and the next ferreting out the weaknesses in new building security gates. "There's always something new to learn," he says.

LAUREN TROMPP

" I GET PAID TO TRY AND BREAK THINGS!"

9am
Review what I'm testing for the day – usually it is a new piece of software or hardware that is ready to be rolled out, which we need to assess. Since the start of the COVID-19 pandemic, I mostly work from home and only go into the office to do certain tasks like hardware testing.

10.30am
After the morning coffee run, I start testing a piece of hardware or software to see if it's working as expected. I collaborate with specialists in various fields during the testing process to detect security flaws. The most common fields are web applications, mobile apps, ATMs and terminals. There are also thick-client applications, which are computer programs rather than apps – like what tellers use to take customer details.

1pm
Lunch! Chicken laksa is my favourite.

2pm
Hardware testing. I use little gadgets to probe the hardware and understand how it is working physically. I also try to eavesdrop on communications between hardware devices, to see if I can extract or tamper with them.

5.30pm
We have a fantastic foosball table at work. Before pandemic restrictions, the team liked to end the day with a game or two. *– Nadine Cranenburgh*

CYBER SECURITY ASSOCIATE, CBA

PEN TESTER, CBA

GRADUATE PROGRAM, CBA

SOFTWARE ENGINEER, PEPPER FINANCIAL SERVICES

BACHELOR OF SOFTWARE ENGINEERING, UNIVERSITY OF SYDNEY

Securing your passion

EVANGELINE ENDACOTT
CYBER SECURITY STUDENT

WHEN EVANGELINE ENDACOTT SCORED THE SECOND TOP MARKS IN HER RURAL HIGH SCHOOL SHE DEFIED EXPECTATIONS TO FOLLOW HER PASSION

Evangeline's great marks meant people in her hometown of Mudgee, NSW expected she would study law. Instead, she enrolled in a computer science (CS) degree at UNSW to pursue her passion for problem-solving.

While she hadn't focused on coding at school, Evangeline was fascinated by the inner workings of tech. "I was always thinking 'how does this work, how does it send information back?'" she says.

Now in her third year of uni Evangeline is majoring in security engineering with a minor in psychology and works two days a week in the Commonwealth Bank of Australia's (CBA) Cyber Security Associate Program.

Evangeline's psychology minor has helped her take an empathetic human approach to cyber security, where she looks at situations "with two minds". It's also given her a lot of practice with report writing, an important part of her cyber security role.

CAT AND MOUSE!

While ethical hacking or pen testing is one of the best-known jobs in cyber security, Evangeline says there is a lot more to the field.

She explains that cyber security roles usually fall into two main areas: the red team (or the pretend bad guys) and the blue team (the good guys). "It's a cat and mouse game," says Evangeline.

Her current role at CBA is with cyber defence operations, which detects malicious activities. She says this is actually a 'purple team',

Red vs Blue

Would you prefer to think like a hacker on the red team, or save the day with the blue team? Or maybe a bit of both with the purple team? Here are a few options:

• **Red team: imitates real-world attacks against the organisation**

• **Purple team: combines the attack and defence team to uplift remediation**

• **Blue team: detects malicious activities and reports for analysis; analyses the impact of the attack; responds by fixing the damage done by attackers**

because it integrates elements of red and blue. "There are so many options out there," she says.

LOVE AT FIRST BYTE

Evangeline discovered security engineering in her second year of uni and fell in love. One of her guest tutors was a member of the CBA cyber security outreach program, who encouraged her to apply for the bank's Cyber Security Associate Program.

After finishing her degree, Evangeline is looking forward to joining the CBA Enterprise Services Graduate Program.

"I'm keen to explore all the opportunities available to me at the CBA," she says. — *Nadine Cranenburgh*

CYBER SECURITY ASSOCIATE, CBA

LAB ASSISTANT AND TUTOR, UNSW

BACHELOR OF SCIENCE (COMPUTER SCIENCE), UNSW

LAUREN TROMPP

THERE ARE SO MANY OPTIONS OUT THERE"

CYBER SECURITY

Schools Cyber Security Challenges

From social media sleuthing to crafty cryptography, the Schools Cyber Security Challenges help students gain skills and knowledge about cyber security practices and principles

The Schools Cyber Security Challenges are a series of realistic learning modules that teach cyber security techniques and coding. They're a great way to skill up in the technical fields and human aspects of cyber security and can be done in groups in class, or solo at home. Challenges can take between four to eight hours to complete.

"We know many schools have programs in cyber safety and bullying, but kids aren't learning the technology elements they need to stay safe," says Associate Professor James Curran, Director of the Australian Computing Academy (ACA), which created and runs the Challenges.

The Challenges cover four topic areas: information privacy and security, data encryption and transmission, wired and wireless network security and web application security. Each Challenge is linked to school learning areas such as Information and Communication Technology (ICT) capabilities and the Australian Curriculum: Digital Technologies.

"As teachers, we were looking for something more than just the usual talks and videos about using social media and the cyber security course has filled this void beautifully," says Shirley

JAMES CURRAN
ASSOCIATE PROFESSOR

Munro, an ICT teacher from McKinnon Secondary College in Melbourne.

"The course is giving students a great insight into the world of cyber security. It shows them how the information they share across different platforms can be pieced together to gather a detailed profile about them in the online world."

More than 85,000 students in 2200 schools from across Australia have taken part in the Challenges. Beren Horgan, a year 7 student at Sydney Secondary College in Balmain says the Information Privacy and Security Challenge was "fun and interactive".

"It was very innovative. They have many different apps to interact with that allow you to find out information about people," he says.

From Cyber 101 to network security

"Students quickly realise how the Challenges relate to unsafe situations and behaviour online by themselves or their parents that leave them open to fraud, cyber attacks or scams," says James.

For example, parents posting about their children's birthdays a few days after the event and posting images of their school uniforms on social media means their personal information is easily accessible. Understanding how much we share online and what's safe and what's risky is a big part of the first Challenge.

"There are little steps people can take to share safely," says James.

> **THERE ARE LITTLE STEPS PEOPLE CAN TAKE TO SHARE SAFELY"**

Test yourself!

Can you decode this word?

D-Z-C-F-S

Hint: take a step forward to see if you can deCIPHER the word. Answer is on p19.

The content is continually updated to stay relevant. For example, while phishing (email scams) is included in the Information Privacy and Security Challenge, there's been a rise in 'SMSishing' or SMS phishing: texts sent directly to kids' phones via SMS.

Skill up for career preparedness

You'll also hear from people working in cyber security, one of the fastest growing job areas around. Worldwide, 53% of organisations report a shortage of cyber security skills. And it's not just about your technical knowhow. Essential cyber security skills include tenacity, curiosity, being systematic, being able to piece together information and being resilient in your approach to a problem, says James.

"All of cyber security is about problem-solving – often with people. If you don't have access to the code on a website and you're looking for a bug (error), you need to think about how you can keep 'pulling that thread' to find that bug," he says.

"We wanted to show in an authentic way that careers link to the kind of problem-solving that you see in the challenges – like social media sleuthing," says James. "In all of our activities we include industry professionals explaining what it's like to work in cyber security. Young people in the working world talking about their career and their pathway is an important insight into what cyber security is."

If you're looking to develop your tech skills further, there are also Digital Technologies Challenges (online and unplugged classroom activities for Years 3–8) and more courses on the ACA website.

Done the Challenges and looking for what's next? You can get involved in Capture the Flag competitions (see p16) or take our cyber safety quiz at bit.ly/cyber-quiz.

"There are a bunch of competitions and activities out there for kids to get into!" says James. – *Heather Catchpole*

NAME DROP
GET THE LINGO

Bug: An error in programming.

Cipher: An algorithm (set of rules) to encrypt or decrypt information. The simplest ciphers replace alphabetical letters with numbers, for example.

Cryptography: Techniques to keep information secure by using codes, scrambling techniques and keys.

Exploit: An attempt to take advantage of a bug or flaw in a system for malicious purposes.

Network security: Rules and set-ups designed to protect networked devices from hacks. Networked devices can include drones, fridges, TVs, road signs, or even vehicles.

Phishing: An attempt to get you to provide information that can be used for cyber crimes like banking details, personal information or passwords.

SMSishing: Phishing scams conducted by SMS.

TRY THESE CHALLENGES!

Information privacy and security

Grasp personal information security by thinking like a hacker. You will learn to value the importance of password strength and protection, as well as discovering just how vulnerable private information can be online.

Cryptography

Learn basic cryptography concepts in relation to data representation and securing online communication, and how these concepts are implemented through code. This Challenge teaches programming in the context of classic cryptographic ciphers like rotation, XOR and mixed substitution, and explains the techniques used to break these forms of encryption.

Network security

This Challenge teaches the fundamentals of wired and wireless networks and the underlying principles of digital systems using BBC micro:bits.

Web application security

This Challenge demonstrates the importance of security in web applications by exposing typical flaws in websites that can be exploited using tools built into the web browser.
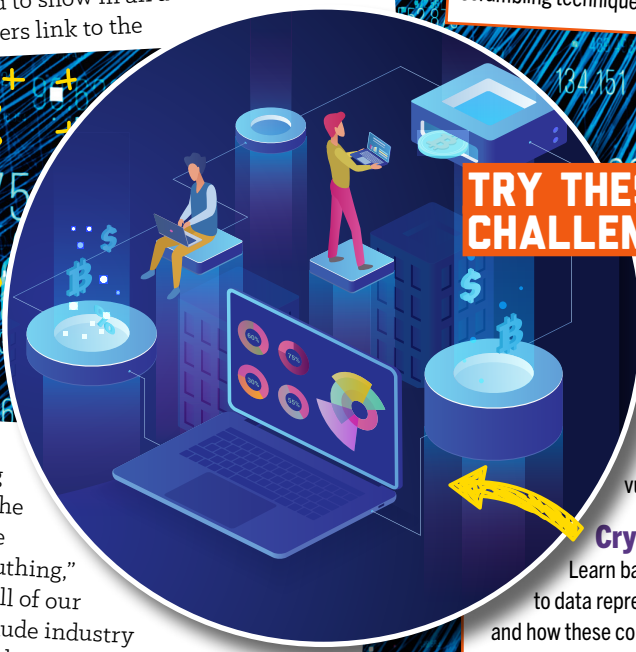
CYBER SECURITY

Myth-busting cyber security careers

Forget what you think you know about a career in cyber security! These five real-life cyber security pros are spilling the facts... and there's hardly a hoodie in sight!

#1

ALISON KIDD
JUNIOR CYBER SECURITY ANALYST, CBA

MTYH: YOU HAVE TO KNOW WHAT YOUR CAREER PATH LOOKS LIKE
FACT: CYBER SECURITY CAREERS ARE WIDE AND VARIED – DISCOVER WHAT YOU LIKE AS YOU FORGE YOUR OWN CAREER PATH

Technology was Alison's favourite subject at school and she knew she wanted a career in tech, so she enrolled at Macquarie University to study a Bachelor of IT majoring in Software Technology. During her degree, a cyber security internship at NSW Health popped up – this was the first time she'd tried it out and she loved it.

Alison switched into the then-brand-new cyber security major at her uni. A Kamilaroi woman, Alison soon found out about another internship opportunity through Walanga Muru, Macquarie University's pathway and engagement program for Aboriginal and Torres Strait Islander students. The internship was at the Commonwealth Bank of Australia (CBA) – and Alison continues to intern part-time as a junior cyber security analyst while completing her degree.

However, Alison is still figuring out exactly where in cyber security she wants to take her career. She currently likes the idea of learning more about penetration testing (pen testing) – the cool-sounding cyber security gig that basically involves finding an organisation's weak spots before someone else does. "It's fun – you're kind of like a hacker, but not really," she says.

Alison expressed this interest to her team at CBA, and now she gets regular tutoring on a Friday. "That's something our team is really great for," she says.

BACHELOR OF IT (CYBER SECURITY), MACQUARIE UNIVERSITY >>> CYBER SECURITY CADET, EHEALTH NSW >>> INTERN, CBA >>> JUNIOR CYBER SECURITY ANALYST, CBA

SHUTTERSTOCK

#2 ANNELISE RALEVSKA
INFORMATION SECURITY CONSULTANT, WESTPAC

Annelise works in Westpac's Security Assessment Services team, which she explains "is pretty much the red team". In cyber security the red team tests the readiness of a company by looking for weak points in computer systems, networks, staff and/or processes. They attack systems, bad processes and procedures, and people's bad habits (like opening fake emails).

For example, Annelise might try to uncover weakness in the bank's security processes by requesting access to a building without the right pass, being as persistent as a real imposter.

Annelise, who started at Westpac as a Young Technologists Scholar, stresses that cyber security is a huge area – and it's not all coding. "There are heaps of different roles in cyber security – you might enjoy more of the creative side, like creating a video campaign to explain what spear phishing is," says Annelise. (Spear phishing is when an attacker sends targeted, fraudulent emails to try and gain access to an organisation's confidential information.)

Annelise says she likes cyber security because it can

MYTH: CYBER SECURITY IS ALWAYS TECHNICAL
FACT: THEY'RE NOT ALL HACKERS AND CODING IS NOT A PREREQUISITE!

be technical, but also creative and strategic, and because it's such important work.

"You have that sense of purpose, you're protecting Australians' money, so it's really important and you're driven to succeed," she says.

BACHELOR OF BUSINESS / BACHELOR OF SCIENCE (IT), UTS >> WESTPAC YOUNG TECHNOLOGIST SCHOLAR >> GRADUATE, WESTPAC

INFORMATION SECURITY CONSULTANT, WESTPAC >> MASTER OF CYBER SECURITY, UNSW CANBERRA

#3 JOE BINDLEY
SECURITY ANALYST, NAB

As a security analyst at NAB, it's Joe's job to manage the security of the accounts of employees with privileged access to internal software and programs.

"Different accounts have different levels of risk associated with them, so you have to be able to understand that and decide which set of procedures you use," explains Joe, adding that this work requires someone who is good at looking at the details and investigating.

As a man on the autism spectrum, Joe brings these skills and more to NAB's cyber security team as part of the bank's neurodiversity program. "If you have people with different ways of thinking, you can often get different approaches to solving problems," says Joe.
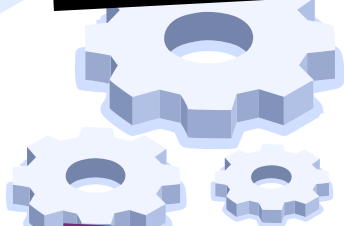
While studying a Bachelor of IT at Deakin University, Joe joined a company called DXC Technology as part of their DXC Dandelion Program, which is about supporting and celebrating the talents and skills of people on the autism spectrum, helping people like Joe build a career in IT.

Through the DXC Dandelion Program, the opportunity arose for a cyber security role at NAB. While Joe's employment is through the Neurodiversity at Work program at NAB, it doesn't define his day-to-day job. "People don't care whether you're autistic or not. If you're good enough, if you're capable to do the job, that's what matters," he says.

MTYH: THERE'S NO ROOM FOR DIVERSITY
FACT: DIVERSE CHALLENGES REQUIRE DIVERSE SOLUTIONS!

BACHELOR OF IT, DEAKIN UNIVERSITY >> DXC DANDELION PROGRAM, DXC TECHNOLOGY >> SECURITY ANALYST, NAB

CYBER SECURITY

#4

ALICE MCCRACKEN
CYBER THREAT INTELLIGENCE ANALYST, ANZ

MYTH: CYBER SECURITY IS AN ANTISOCIAL BOYS' CLUB
FACT: YOU CAN SEEK OUT SOCIAL SPACES AND SUPPORT GROUPS

Alice knew she wanted to study something tech-related at uni, but she also wanted to make sure her career had a deeper sense of purpose and job satisfaction. When she came across the Bachelor of Cyber Security at La Trobe University in Melbourne it looked like the perfect match.

"For me, cyber security has that deeper sense of purpose beyond your average networking and programming sort of stuff," says Alice.

However at uni, Alice found herself to be one of only a few women in the course. "We started hanging out between classes, and we realised we all felt, if not exactly imposter syndrome, then a little bit out of place in a male-dominated course," she says. So Alice and her friends started up a support network called Girl Code. "We wanted to create a safe space to have a study group or a Facebook support page where we could ask questions that we didn't always feel comfortable asking in a formal learning environment."

At the start of this year, Alice undertook a two-month summer internship at ANZ bank, which turned into a regular part-time gig as a threat intelligence analyst while she finishes her degree.

When she graduates, Alice says she's keen to be involved with similar support networks to Girl Code, but for cyber security professionals — such as the Australian Women in Security Network.

SHUTTERSTOCK

BACHELOR OF CYBER SECURITY, LA TROBE UNIVERSITY >> **TECH INTERN, ANZ** >> **THREAT INTELLIGENCE ANALYST, ANZ**

#5 BENJAMIN FERLAUTO
SECURITY THREAT INTELLIGENCE ANALYST, BT

Benjamin says he's had ambitions for a career in cyber security since he was very young. "I enjoy being challenged and I'm always willing to learn or adapt to change. Cyber security is an industry that is constantly evolving and offering exactly that," he says.

Benjamin signed up for a Bachelor of Science in Information Technology, majoring in Cyber Security at the University of Technology, Sydney. He's still in his fourth year at uni, but is already working in the industry, playing a key role testing and launching the new Threat

MYTH: YOU HAVE TO BE FULLY QUALIFIED BEFORE YOU CAN WORK IN CYBER SECURITY
FACT: YOU CAN LAND A JOB WHILE YOU STUDY!

Intelligence Service at global telecommunications company BT, where he works part-time.

"I'm one of a number of people leading the Threat Intelligence Service which will be released as a global service offered by BT," explains Benjamin. Under the new service, BT will provide organisations with information about the current and emerging cyber security threats and deliver real-time intelligence, helping them stay ahead of cyber criminals.

Benjamin first landed a cyber security internship at BT through the UTS CareerHub, which helps students find industry experience opportunities. The internship then turned into a part-time gig while Benjamin simultaneously finishes his degree.

When Benjamin's not working and studying, he loves gaming. In fact, he spent two years working for US professional gaming company, eRa Eternity, before retiring from the pro-gaming world to focus on his study and cyber security career. — *Gemma Chilton*

BACHELOR OF SCIENCE IN IT (CYBER SECURITY), UTS >> SECURITY ANALYST INTERN, BT >> THREAT INTELLIGENCE ANALYST, BT

CYBER SECURITY

THE ROAD LESS TRAVELLED

These four experts all work for one of the world's biggest cyber security companies — but took very different paths to get there

Palo Alto Networks is a global cyber security company. It creates and sells cyber security technology and solutions to more than 70,000 organisations and 150 countries.

#1 TAFE grad with a passion for acting

Jason Spindlow says he finished high school with "average marks". He dreamed of becoming an actor, but felt he needed a fallback job. He signed up for a Cert IV in Tech Support at TAFE, then moved into IT Palo Alto Networks, which means he assists and educates IT companies that sell Palo Alto Networks cyber security technologies and solutions. Now he's a channel systems engineer at cyber security technologies and solutions. Jason also performs in theatre and musicals. "All of these experiences can come into play with how we view and present the cyber security discussion," he says.

CERT IV TECHNICAL SUPPORT (IT), TAFE >> NETWORK ENGINEER, CYBERPRO >> ADVANCED DIPLOMA IN NETWORK SECURITY, TAFE >> CHANNEL SYSTEMS ENGINEER, PALO ALTO NETWORKS

#2 Law grad

Amy Finer studied a Bachelor of Laws at the University of Manchester in the UK and spent a few years working in the legal industry before she decided she was interested in cyber security. "I knew after my law degree that I wanted to work in cyber security. I understood how the threat landscape was changing and the challenges this presented to organisations," says Amy. Now she works as a territory sales manager for Palo Alto Networks, selling Palo Alto Networks technology and solutions, conducting sales training and planning industry marketing events. "I love working in the cyber security industry. I learn something new every day," she says.
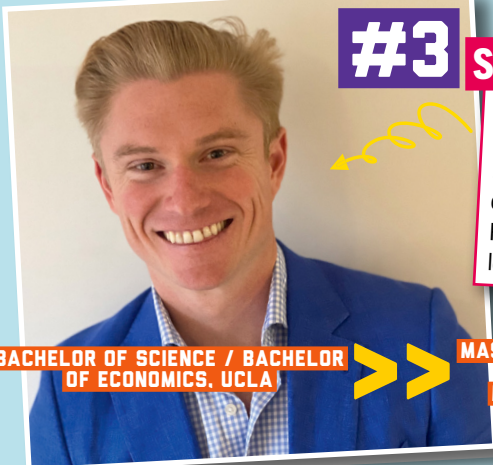
BACHELOR OF LAWS, UNIVERSITY OF MANCHESTER >> SENIOR CASE MANAGER, CYFOR >> CUSTOMER SUCCESS MANAGER, WANDERA >> TERRITORY SALES MANAGER, PALO ALTO NETWORKS

#3 Systems engineer with a background in military technology

US grad **Damien Lewke** started his career as a nuclear weapons engineer for one of the world's largest military technology companies, Northrop Grumman. While he was working there and completing his Masters in Systems Engineering, America's Democratic Party was hacked. "I realised the far-reaching impacts of cyber espionage," says Damien. He left Northrop Grumman, eventually landing his Australia-based role at Palo Alto Networks as a systems engineer. "There's no such thing as a boring day! You're constantly learning from and working with people to tackle security. It's the best job — hands-down!" he says.

BACHELOR OF SCIENCE / BACHELOR OF ECONOMICS, UCLA >> MASTER OF SCIENCE (SYSTEMS ENGINEERING), LOYOLA MARYMOUNT UNIVERSITY >> SYSTEMS ENGINEER, NORTHROP GRUMMAN >> SYSTEMS ENGINEER, PALO ALTO NETWORKS

#4 Telecommunications and networking engineer

Nishita Shetty studied a Bachelor of Engineering with majors in Electronics and Telecommunications in India, spending several years in networking roles. "I was curious to learn cyber security," she says. When Nishita moved from India to Australia, she took on the challenge of a new career as well as a new country. "My networking background helped me to learn quickly and that's how I landed here in the exciting world of cyber security," says Nishita, who works as a systems engineer at Palo Alto Networks. "There is nothing more satisfying than helping a customer solve security challenges," she says. – *Gemma Chilton*

BACHELOR OF ENGINEERING (ELECTRONICS AND TELECOMMUNICATIONS), BHARATI VIDYAPEETH >> MASTERS IN INFORMATION MANAGEMENT, WELINGKARS INSTITUTE >> NETWORK SPECIALIST, APARA >> SYSTEMS ENGINEER, PALO ALTO NETWORKS

TEST YOUR CYBER SKILLS

LOVE PLAYING GAMES AND SOLVING PUZZLES? PIT THEIR WITS AGAINST INTRIGUING CYBER CHALLENGES. OH. AND ALSO GET ENDLESS SOFT DRINKS AND PIZZA

In a Cyber Security Challenge you must decrypt, decipher, break and hack your way through a series of goals, typically gaining 'flags' at each point.

This can mean solving number or word puzzles, going into the code behind websites or images, cryptography, searching through posts for clues and even using ethical hacking practices to locate real-world missing people, as was the case in a recent Western Australian Capture the Flag (WACTF) event.

"All of the challenges presented are built off real-world scenarios that Perth security practitioners have come across," says Aaron Doggett, one of the organisers of WACTF and director of cyber security consultancy Hivint.

"The aim isn't to expose people to theoretical problems, but to show them the types of things that penetration testers, analysts, forensics consultants

Solving crime in the cyber security world makes for hungry work. Lucky there's pizza!

ALL OF THE CHALLENGES PRESENTED ARE BUILT OFF REAL-WORLD SCENARIOS"

and more face. So, if you enjoy what you see, you may well like the career path too," he says.

The two-day event brings high school, TAFE and uni students together with IT professionals, or those with an interest in IT.
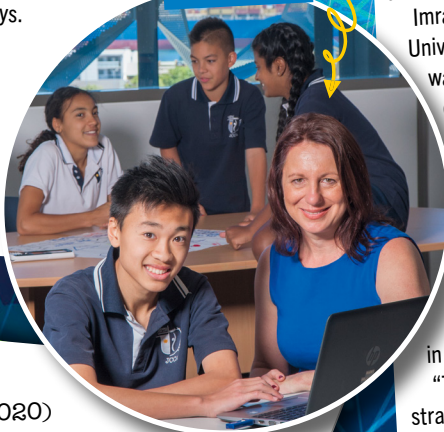
"WACTF also promotes teamwork and the bringing together of people with different skills, approaches and general perspective," says Aaron.

LIKE A CHALLENGE?

Perth teacher Donna Buckley, Assistant Head of Mathematics at John Curtin College of the Arts says students were very engaged. "It wasn't always the kids who did well in tests – critical thinking, curiosity and persistence were some of the skills they really needed," Donna says.

High school student Orlando Morris-Johnson from Perth Modern School has done two CTF events. "You work on everything hacking-wise: reverse engineering programs, breaking encryption and much more," Orlando says.

DONNA BUCKLEY EDUCATOR

There's a host of cyber security challenges to look out for. Daisy Sinclair is founder and CEO of Cyber8Lab one of the companies that runs the Regional Cyber Challenge – an event that pits international teams against hypothetical attackers in an Incident Response Challenge.

"The Regional Cyber Challenge gives you invaluable experience which demonstrates hands-on processes required to respond to cyber attack and defending your network at the same time," Daisy says.

Imran Esack Dawoodjee from Asia Pacific University of Technology and Innovation, Malaysia was on 2019's winning team, Shellhound. "The challenges themselves provided to us during the competition were *very* interesting, employing a mix of skills from different disciplines in cyber security," says Imran.

"For example we were asked to analyse an email that was possibly malicious," he says. "Digital forensics, malware analysis and software reverse engineering all came in handy while solving that challenge."

"The human side of things is not so straightforward and much more insidious: for every wrong flag we submitted, we'd have marks deducted," Imran explains. "It really hammered home that defenders can't afford to make mistakes lest more people be hurt." – *Heather Catchpole*

Find a Challenge!
- WACTF: capture.tf (12–13 Dec 2020)
- AustCyber: bit.ly/austcyber-challenges
- CSIRO's CyberTaipan: digitalcareers.csiro.au/en/CTaipan
- Regional CyberChallange: regionalcyberchallenge.com

How not to overshare online

The lowdown on what's OK to post on socials and what you should keep to yourself

It might seem obvious not to share your bank details online – but surely a pic of you in your school uniform is harmless? How about checking in online when you're at your favourite local cafe with mates?

It's not always super clear how your online information can be used – for example, your school uniform probably has a logo on it that can be used to locate your school and therefore identify you (because you're likely the only person with your exact full name at your school).

Similarly, getting excited about holidays on socials is fun, but you could also be advertising that your house will be empty. Here's a #TMI checklist to staying secure...

✔ OK TO SHARE
Some of the following might help narrow down your identity, but probably won't be enough to identify you.

- Your full name
- Your nickname
- The weather
- GIFs
- Memes
- Your sports and hobbies
- Your pet's name

! SHARE WITH CAUTION
These are usually OK to share, but think twice about how much information you're giving away and to whom – you may want to limit the following to people you trust.

- Birthday
- Photos
- Mobile number
- Geotagged photos
- Holiday plans
- Email address
- Pic of concert tickets
- Check-in location
- Your school

✘ DON'T SHARE
Keep these deets top secret – you don't want them getting into the wrong hands!

- Home address
- Banking PIN
- Login and password details
- Banking details
- Pic of your new driver's licence

Challenge yourself! This info is taken from just one of many resources and activities available through the Australian Computing Academy (ACA), which offers Digital Technologies and Cyber Security Challenges online for you to test your tech and cyber skills! **Visit aca.edu.au for more.**

SHUTTERSTOCK

CYBER SECURITY

CYBER SECURITY JOBS NEED YOU!

ONE OF AUSTRALIA'S TOP CYBER SECURITY EXPERTS, PAUL HASKELL-DOWLAND, GIVES US THE LOWDOWN ON THE WORLD'S MASSIVE SKILLS SHORTAGE IN CYBER SECURITY – AND WHY THAT MEANS BIG CAREER POTENTIAL

Cyber security jobs are diverse, challenging and exciting – and there is no where near enough people signing up for the career, which means huge opportunity, according to Associate Professor Paul Haskell-Dowland, a cyber security expert at Edith Cowan University (ECU). With more than 20 years in the industry in Australia and the UK, he should know.

"The capacity of schools, TAFEs and universities to deliver the number of people that's needed with the skills required in industry is not going to catch up for many years," Paul says. "We're looking globally at hundreds of thousands of jobs unfilled, rising to millions, this decade."

For example, Paul says ECU alone has over 1100 students studying cyber security – and that's just in ECU's dedicated courses, not

PAUL HASKELL-DOWLAND
ASSOCIATE DEAN OF COMPUTING AND SECURITY

those taking cyber majors and units. "We're generating enormous numbers of students in the area of cyber security and we're barely touching the tip of the iceberg," he says.

The ongoing skills shortage puts graduates in high demand which pushes up salaries. "We tell students that your first job will come off the back of your degree and promoting yourself to the industry, but your second and third jobs will come calling for you," Paul says.

His advice for the cyber security professionals of the future? "Working in cyber draws on a wide skill set, but you don't need a technology background to come into cyber security. Really, it's having that flair, that enthusiasm that matters," he says. – *Gemma Chilton*

SHUTTERSTOCK

SEE YOURSELF ON THE FRONTLINE OF CYBER SECURITY

**Study at WA's only Academic Centre of Cyber Security Excellence.**

With cyber security threats only increasing, there's never been a greater need to protect Australian businesses, government and the community from digital crimes.

ECU's cyber security courses are designed to meet the changing landscape of our cyber security future. Our students learn in world class facilities, including a new multimillion dollar Security Operations Centre opened in 2020. They also receive real world experience through placements, internships and industry projects making them ready to tackle a constantly changing digital world.

ECU has the largest cyber security and research program in Australia, which has been recognised by the Australian Federal Government as one of just two Academic Centres of Cyber Security Excellence in Australia. For an in-demand career in a fast growing industry, study cyber security at ECU.

APPLY NOW
ECUWORLDREADY.COM.AU/CYBER-SECURITY

AUSTRALIA
ECU
EDITH COWAN
UNIVERSITY
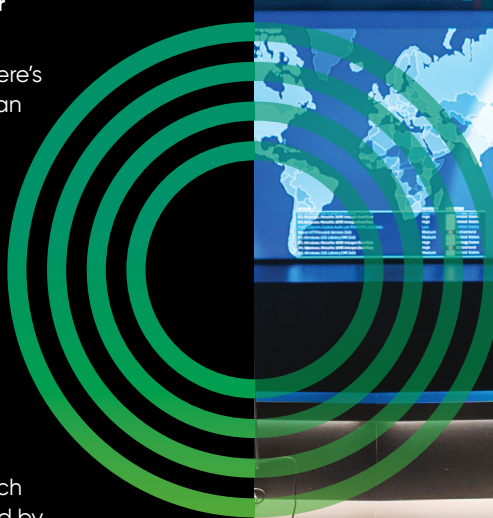
WHAT SHOULD I STUDY?

THERE'S PLENTY OF OPTIONS OUT THERE... FROM SHORT TASTER COURSES TO SPECIALIST DEGREES IF YOU'RE THINKING A CYBER CAREER MIGHT BE FOR YOU.

OPTION #1:
DO AN ENGINEERING, SCIENCE OR IT DEGREE AND SPECIALISE

>> Bachelor of Science (Cyber Security), **Edith Cowan University**
>> Bachelor of IT (majoring in Cyber Security), **Macquarie University**
>> Bachelor of Networking (majoring in Cyber Security), **Melbourne Institute of Technology**
>> Bachelor of Computing and Cyber Security, **UNSW**
>> Bachelor of Cyber Security and Behaviour, **Western Sydney University**

OPTION #2:
DO ANY DEGREE AND THEN DO A POSTGRADUATE DEGREE IN CYBER SECURITY

>> Master of Cyber Security, Strategy and Risk Management, **Australian National University**
>> Master of Cyber Security, **Edith Cowan University**
>> Master of Cyber Security, **University of Queensland**

OPTION #3:
STUDY CERTIFICATE OR SHORTER COURSES THROUGH TAFE OR UNI

>> Certificate IV in Cyber Security, **Melbourne Polytechnic**
>> Graduate Certificate in Cyber Security and Networks, **QUT**
>> Certificate IV in Cyber Security, **TAFE NSW**
>> Associate Degree in Applied Technologies specialising in Cyber Security, **University of Tasmania**

OPTION #4:
DO A CYBER SECURITY BOOT-CAMP COURSE

>> Diploma of Information Technology, 10-month course, **Coder Academy**
>> Cyber Security Program, three-month course (full time), **Institute of Data**
>> Cyber Security Risk and Strategy, six-week course, **RMIT**
>> Cyber Security Boot Camp, five-day course, **UNSW Canberra**
>> Cyber Security Boot Camp, 24-week course, **University of Western Australia**

WHAT CAN I EARN?

|	
CYBER SECURITY ANALYST	AU$56K–$109K
CYBER SECURITY ENGINEER	AU$49–$134K
PEN TESTER	AU$52K–$133K
SECURITY CONSULTANT	AU$87K–$167K*

*Source: salaries according to payscale.com

Decipher to win!

Decipher this to win all the kudos *and* a copy of *Ready, Set, Code!*

sqhuuhi myjx ijuc

Email your answer to info@refractionmedia.com.au with the email subject 'Cyber challenge'. The first correct response will win a copy of *Ready, Set, Code!* from CSIRO Publishing.
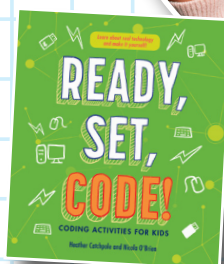
HINT: Make sure you use the right font and enjoy all of the pages of the mag!
For full terms and conditions go to: careerswithstem.com.au/terms-and-conditions

SHUTTERSTOCK

Answer from p8: cyber

CYBER SECURITY