Cybersecurity Mentoring Program:

Exploring Cybersecurity as a Career

Guiding future professionals in digital security fields

Why this session matters and what mentees will gain

Inclusive Cybersecurity Careers

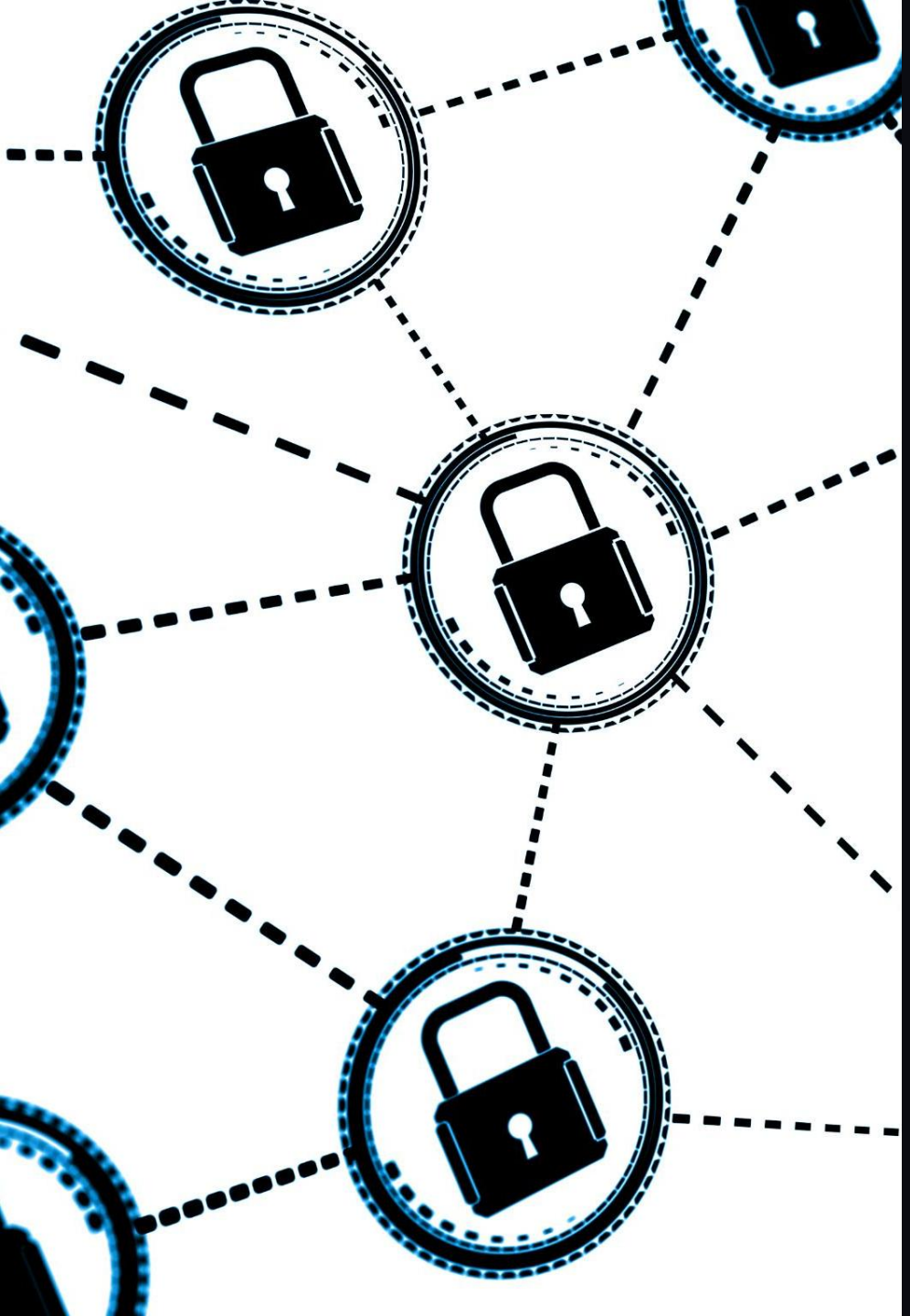
Cybersecurity welcomes diverse skills beyond coding, including problem-solving and communication.

Everyday Relevance

Cybersecurity protects everyday internet activities like banking, gaming, and social media usage.

Session Goals

Understand cybersecurity basics, explore career options, and learn practical first steps without special tools.



WHY CYBERSECURITY — framing the ‘why’ before the ‘what’

Cybersecurity’s Purpose

Cybersecurity protects essential digital systems that impact everyday human activities and maintain trust.

Evolving Threat Landscape

Technology constantly changes and attackers adapt quickly, driving ongoing demand for cybersecurity experts.

Beyond Stopping Attackers

Cybersecurity also ensures systems are resilient, private, and fair through strong controls and governance.

Human Element in Security

People play a critical role by making good decisions and spotting threats, enabling multiple career paths.

Understanding Cybersecurity and Everyday Threats

Cybersecurity’s real-world impact on daily life and public services

Cybersecurity in Daily Technology

Everyday activities like messaging, social media, and online banking rely on secure digital systems to protect user data.

Impact on Public Services

Cyberattacks like ransomware can disrupt essential services such as healthcare, education, and local government operations.

Risks of Account Takeovers

Hacked accounts can lead to scams, privacy breaches, and financial losses, affecting individuals’ safety and trust.

Collaborative Cybersecurity Efforts

Cybersecurity is a team effort involving IT, legal, management, and users to build trust and respond to threats.

Definition and the security cycle: prevent, detect, respond, recover

Prevention Strategies

Prevention includes strong passwords, multi-factor authentication, secure system design, and software updates to patch vulnerabilities.

Detection Methods

Detection involves monitoring unusual activity like unexpected logins, large data downloads, and malware symptoms on devices.

Response Actions

Response includes investigating incidents, containing threats by locking accounts or isolating devices, and coordinating fixes.

Recovery Process

Recovery focuses on restoring services safely, verifying data integrity, and improving controls for stronger security.

Common threats: phishing, password attacks, ransomware, social engineering

THREAT	TYPICAL GOAL	EXAMPLE	COMMON DEFENCES
Phishing	Trick you into clicking or logging in	Fake parcel delivery SMS	Check sender, verify via official app/site
Password attacks	Take over accounts	Reused password from an old site breach	MFA, password manager, unique passwords
Ransomware	Lock systems for money	School files become inaccessible	Backups, patching, least privilege
Social engineering	Manipulate people to bypass controls	"IT" asks for your verification code	Training, verification steps, reporting culture

Recognising manipulation and red flags

PHISHING RED FLAG	WHAT IT LOOKS LIKE	SAFER RESPONSE
Urgency	"Act now" / "Today only" / "Account locked"	Pause; verify via official site/app
Too good to be true	"You've won" / "Free gift" / "Refund"	Assume scam; don't click links
Sender mismatch	Weird email domain or random number	Check sender details carefully
Suspicious links	Shortened URLs, misspellings, odd domains	Type the website yourself
Unexpected attachment	Invoice, document, ZIP file you didn't ask for	Don't open; confirm with sender another way

Myth vs reality: widening access and reducing intimidation

Myth: You Have to Be a Hacker

Most cybersecurity jobs focus on defense, reducing risk, and system monitoring rather than hacking.

Myth: Coding Genius Required

Many cybersecurity roles need analytical thinking and communication more than advanced coding skills.

Myth: You Work Alone

Cybersecurity is highly collaborative, involving IT, legal, leadership, and external partners in incident response.

Encouraging Diverse Backgrounds

Cybersecurity welcomes talents from writing, psychology, law, design, and business; curiosity is key.

Career Paths and What the Work Looks Like

CAREER PATHS — connecting interests to roles

Exploration Over Perfection

Careers are discovered through exploration; you don’t need to pick a perfect role immediately.

Variety of Cybersecurity Roles

Cybersecurity includes investigative, creative, policy-driven, and technical roles matching diverse interests.

Transferable Skills Matter

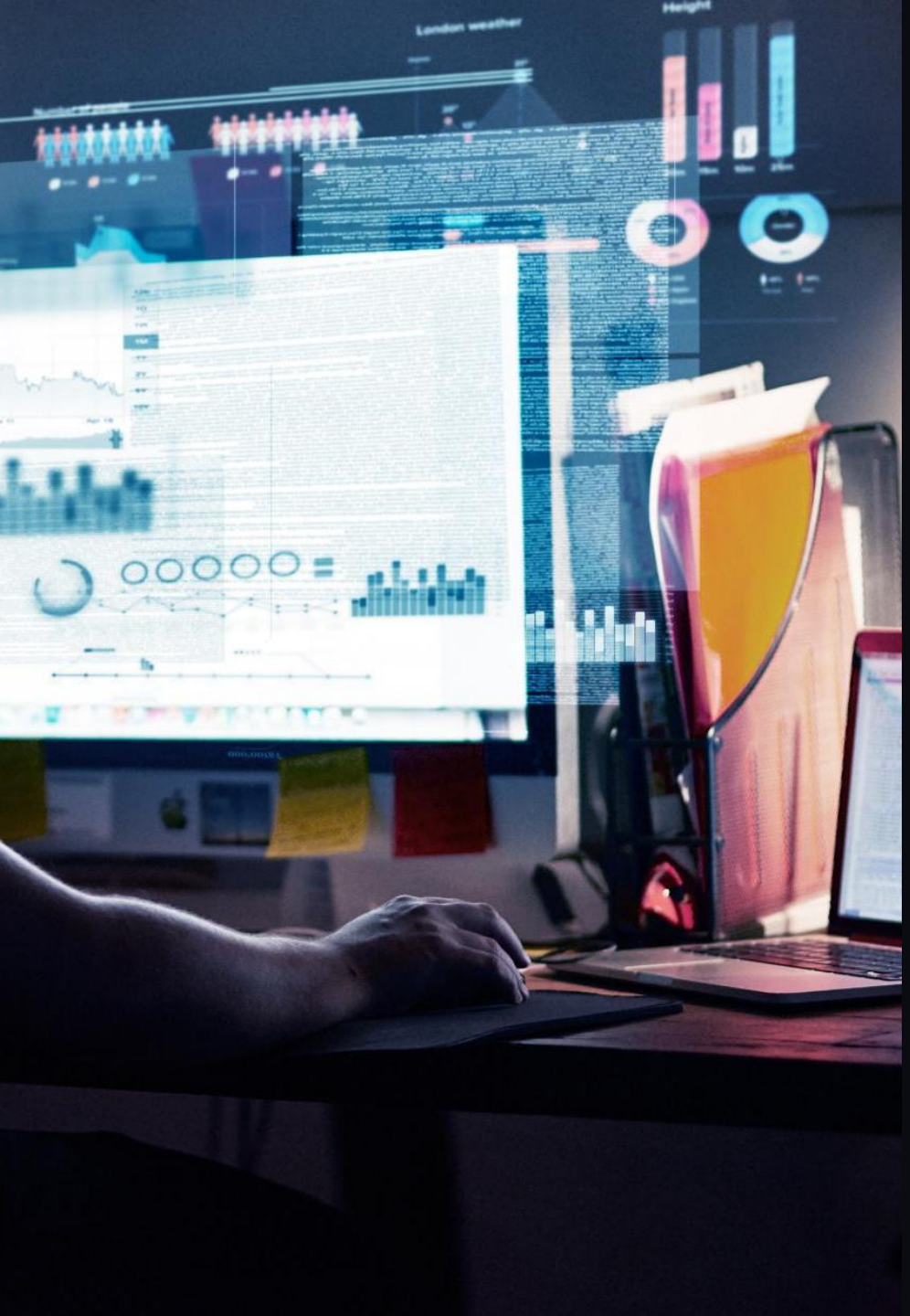
Skills like teamwork, communication, and ethical judgement are valuable across all cybersecurity roles.

Career Outlook

Cybersecurity careers are challenging, meaningful, and accessible through learning and apprenticeships.

Cybersecurity roles overview: SOC, cloud, identity, incident response, GRC

ROLE	CORE FOCUS	TYPICAL TASKS	GOOD FIT IF YOU LIKE...
SOC / Security Analyst	Detect & investigate threats	Triage alerts, investigate logins, escalate incidents	Puzzles, patterns, problem-solving
Cloud Security	Secure cloud systems	Review configurations, manage cloud risks, enforce controls	Building systems, architecture, optimisation
Identity & Access (IAM)	Control who can access what	MFA, permissions, conditional access, account hygiene	Structure, correctness, protecting the “front door”
Incident Response	Contain and recover during attacks	Investigate breaches, isolate devices, restore services	High-impact teamwork, staying calm under pressure
GRC	Risk, policy, compliance	Standards, training, audits, risk registers	Communication, planning, helping organisations improve



Day in the life: Security Analyst story walkthrough

Incident Investigation Process

Security analysts calmly investigate alerts by verifying normal behavior and corroborating evidence for risks.

Decision Making and Containment

Analysts prioritize risks and contain threats by actions like password resets or account blocks to protect systems.

Collaboration and Communication

Effective communication with IT, managers, and users fosters a strong security culture and timely incident response.

Career Progression in Cybersecurity

Entry-level analyst roles build foundational skills that lead to specialization in incident response or threat hunting.

Skills that matter: technical basics plus human strengths and ethics

SKILL AREA	WHAT IT MEANS	HOW MENTEES CAN PRACTICE
Curiosity	Wanting to understand how things work	Ask “why” when apps request permissions
Basic IT knowledge	Accounts, devices, networks, data	Learn fundamentals via free online modules
Critical thinking	Evaluate evidence before acting	Pause-check-verify suspicious messages
Communication	Explain risks clearly to others	Teach a friend how to enable MFA
Ethics	Do the right thing with access and info	Report vulnerabilities responsibly

Getting Started

GETTING STARTED — practical routes and first actions

Multiple Career Routes

Cybersecurity offers multiple entry routes including apprenticeships, degrees, certifications, and self-learning.

Focus on First Steps

Start with basics like networking, safe account habits, and beginner labs instead of final career choices.

Learning Styles and Resilience

Choose a learning style that fits you and build resilience through consistent practice despite challenges.

Motivation and Impact

Cybersecurity careers enable protecting others, solving problems, and continuous improvement over time.

Routes into cybersecurity

ROUTE	WHAT YOU GAIN	BEST FOR	TYPICAL NEXT STEP
College / Sixth Form	Foundations in IT, maths, problem-solving	Structured learning	Apprenticeship or university application
University	Depth, theory, wider networks	Academic learners	Graduate schemes, internships
Apprenticeship	Earn while learning, real experience	Hands-on learners	Junior security/IT roles
Certifications	Evidence of knowledge and commitment	Career starters / switchers	Entry-level roles, further labs
Self-learning + labs	Practical skills and portfolio	Independent learners	Portfolio + applications

Choose one realistic first step in the next 3 months

Online Learning

Short online modules cover basics like networking, internet functions, and security fundamentals.

Trying Labs

Hands-on practice in safe labs builds skills through solving challenges and real security scenarios.

Following Cybersecurity Content

Consuming trustworthy content helps build awareness of scams, privacy, and security habits.

Talking to Mentors

Mentorship provides real-world insights, feedback, and career guidance in cybersecurity.

Ethics and responsibility: trust, legality, and doing the right thing

Trust in Cybersecurity

Cybersecurity professionals earn trust by protecting sensitive data and systems during critical incidents.

Responsible Vulnerability Handling

Exploiting or publicly sharing vulnerabilities harms people and breaks laws; responsible reporting mitigates risks.

Everyday Ethical Practices

Respect privacy, avoid sharing passwords, and do not test accounts without consent to uphold cybersecurity ethics.

Legal Boundaries and Opportunities

Learning is safe in controlled environments; responsible disclosure can open legal opportunities like bug bounties.

Personal Journey

Key takeaways: impact, multiple paths, curiosity over perfection, belonging

Cybersecurity Protects People

Cybersecurity ensures trust and safety for schools, hospitals, businesses, and families, highlighting its human impact.

Diverse Career Paths

Cybersecurity offers many roles like analysts, cloud specialists, and incident responders matching varied interests.

Curiosity Over Perfection

Continuous learning and curiosity are valued more than perfection in the evolving cybersecurity field.

Belonging and Inclusion

Cybersecurity needs diverse perspectives and encourages everyone who cares about protecting others to belong.

Q&A