






## Virtual Work Experience – Trainee Cybersecurity Analyst


### Overview

This virtual work experience is designed to give students real-world insight into the role of a Trainee Cybersecurity Analyst. As part of this experience, students will go through a structured **recruitment process**, similar to what happens in a real business.


By participating in this process, students will:


-  Understand how businesses recruit and select candidates.
-  Gain experience in cyber threat detection and risk analysis.
-  Learn how to use [NCSC Active Cyber Defence \(ACD\)](#) tools to assess and improve school cybersecurity.

### Application Submission

 What to Submit:

- A **personal statement** (Why do you want to be a Trainee Cybersecurity Analyst?).
- Any **relevant skills or experiences** (e.g., problem-solving, data analysis, cybersecurity awareness, coding).

 **Business Insight:** *In a real workplace, employers receive applications and select candidates based on their **skills, motivation, and suitability** for the role.*

 Shortlisting Process:

- All applications are reviewed fairly.
- Shortlisted students move to the **interview stage**.

### Virtual Interview

 Format: A **30-40 minute** online interview.

 Who Will Interview You? A mentor from CyberSafeSchools Academy.

Interview Structure:

#### 1) Introduction & Motivation

- Why are you interested in the Trainee Cybersecurity Analyst role?
- What do you know about CyberSafeSchools Academy?
- Have you ever worked on cybersecurity, coding, or risk analysis projects before?

#### 2) Cyber Awareness & Analytical Thinking


- Why is cybersecurity important for schools?
- What do you understand about cyber threats like phishing, malware, and ransomware?
- Have you ever used cybersecurity tools or conducted any security analysis before?

#### 3) Problem-Solving & Technical Skills

- If a school's website was flagged as having security vulnerabilities, how would you investigate?
- How would you explain cyber threat intelligence to someone unfamiliar with the field?
- What do you know about the role of government cybersecurity agencies like NCSC?

#### 4) Future Goals & Learning

- What do you hope to gain from this experience?
- Do you see yourself working in cybersecurity, ethical hacking, or IT security in the future?

 **Business Insight:** In real-world recruitment, companies assess candidates based on **technical knowledge, analytical thinking, and problem-solving skills**.





### ◆ Scoring Criteria:

- ✓ Technical Curiosity & Initiative
- ✓ Communication & Confidence
- ✓ Cyber Awareness & Threat Understanding
- ✓ Analytical & Problem-Solving Skills

**Next Step:** Successful candidates move to the **task-based assessment** stage.

### Step 3: Task-Based Assessment

 Purpose: To assess technical skills, analytical thinking, and ability to use cybersecurity tools.

 **Business Insight:** Many companies require a task-based assessment to evaluate a candidate's skills before offering a role.

### **Project Task: Cybersecurity Risk Assessment Using NCSC Active Cyber Defence Tools**

Your task is to conduct a basic cybersecurity risk assessment using publicly available [NCSC Active Cyber Defence \(ACD\) tools](#).




### ◆ Task Requirements:

- Research and summarize what the NCSC ACD tools are and how they help protect schools.
- Use the NCSC Web Check tool to identify vulnerabilities in a school's website (or a sample domain).
- Use the Mail Check tool to assess the security of a school's email domain.
- Provide a brief report on findings, potential risks, and recommended actions.

### ◆ Submission Format:

 Technical Report (Google Docs, Word) OR  Slide Presentation (Google Slides, PowerPoint)

### Assessment Focus:


-  Technical Accuracy & Research Skills
-  Problem-Solving & Risk Analysis
-  Ability to Use Cybersecurity Tools

---

### ✓ **Final Selection & Confirmation**

 Successful applicants receive:

- A confirmation email welcoming them to the Virtual Work Experience.
- Their assigned mentor and project details.

 **Business Insight:** After assessments, businesses select the best-fit candidates based on technical ability, analytical skills, and cybersecurity knowledge.


### ◆ Unsuccessful applicants:

- Receive constructive feedback.
- Encouraged to reapply in the future.




### Virtual Work Experience Structure Overview

- ◆ Induction & Training – Meet mentors, learn about CyberSafeSchools, and set goals.
- ◆ Project Work – Conduct cybersecurity risk analysis using NCSC ACD tools and document.
- ◆ Mentor Feedback & Skills Development – Learn about cybersecurity careers and risk assessment methodologies.
- ◆ Final Presentation – Showcase your findings and recommendations.

 **Business Insight:** A Trainee Cybersecurity Analyst must be able to identify risks, analyse security threats, and recommend mitigations using industry-standard tools.

### Post-Work Experience Activities

- ◆ Offboarding Process – Understanding how cybersecurity analysts transition out of roles.
- ◆ Exit Interviews – Provide feedback on the experience and discuss future opportunities.
- ◆ Reference & Certification – Receive a certificate of participation and potential reference for future roles.
- ◆ Networking & Alumni Connection – Stay connected with CyberSafeSchools Academy for future opportunities.

 **Business Insight:** Just as onboarding is crucial, the exit process ensures a smooth transition and future career opportunities for employees.

### Key Takeaways for Students

- ✓ Experience a real hiring process similar to business recruitment.
- ✓ Develop technical and analytical cybersecurity skills.
- ✓ Gain hands-on experience with NCSC Active Cyber Defence tools.
- ✓ Work with a mentor and present a real-world cybersecurity risk assessment.
- ✓ Understand the offboarding process and its importance in a career journey.