THE CYBER **SCHEME**

®

STARTING YOUR CAREER IN CYBER

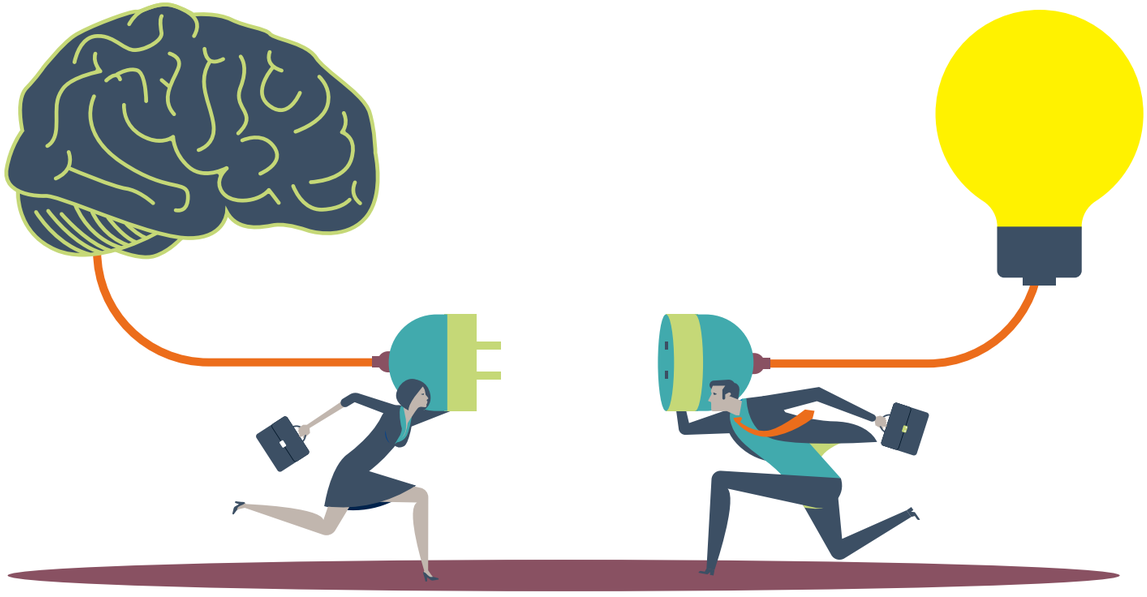
"If you are just starting your career in cyber security, it can be a confusing journey. There are countless certifications, training organisations and 'must have requirements', and it's not easy to navigate which path to take - even if you already have a formal academic qualification in cyber security.

The Cyber Scheme are committed to aiding those who have chosen this career path in gaining their first job - whether straight out of education, or re-skilling from another vocation.

This brochure has been created to help you identify the best choices for you - but please note, it's not a definitive list. In order to succeed in a career in cyber security, you must love to learn - your career will be demanding, ever changing and constantly developing as new threats evolve. It's what makes a job in cyber security so rewarding - but you do need to commit time and effort and be prepared to self-learn and self-assess every step of the way.

You'll need to stand out if you want to gain a foothold at entry level; this brochure should be the first step in making sure you have what employers are looking for. Don't rely on Google to help you - instead research, find mentors in industry, ask questions, and above all gain practical experience. Then you'll be on your way.

Good luck!"



Steps to Success:

1. Determine which area of cyber security you want to enter.

DO NOT tell employers or recruiters you wish to 'get into cyber' or that you don't mind which area you start in. Different specialisms require very different skill sets, and it's vital that you choose an area which fits yours, and stick to it. Being single minded at this point will help you stay focussed when choosing learning pathways and certifications; collecting a bunch of unrelated certs and training qualifications gives the impression you're not yet sure what you want to do. Aim for fewer, higher quality certifications, and get advice before you buy any (more on that later).

It is our belief at The Cyber Scheme that prospective candidates should wherever possible conduct their own research into which field of cyber security they wish to enter. This signifies to a would-be employer that you have the required curiosity, research capability and independent thought that is needed. Candidates who can say they have identified a specialism that meets their skills - whether it's technical capabilities, or an interest in ethics and law - will stand out at application and interview.

So your first step on this journey is to conduct self-analysis of your own skills and interests, including an honest appraisal of how technical you are or wish to be, and map your skills against recognised cyber specialisms and job roles.

Need help choosing? The following are recognised as the 16 specialisms within cyber by the UK Cyber Security Council:

- **Cryptography & Communications Security**
- **Cyber Security Audit & Assurance**
- **Cyber Security Generalist**
- **Cyber Security Management**
- **Cyber Threat Intelligence**
- **Data Protection and Privacy**
- **Digital Forensics**
- **Governance and Risk Management**
- **Identity & Access Management**
- **Incident Response**
- **Network Monitoring & Intrusion Detection**
- **Secure Operations**
- **Secure System Architecture & Design**
- **Secure System Development**
- **Security Testing**
- **Vulnerability Management**

For further guidance on each of these specialisms, please click here.

2. Find mentors.

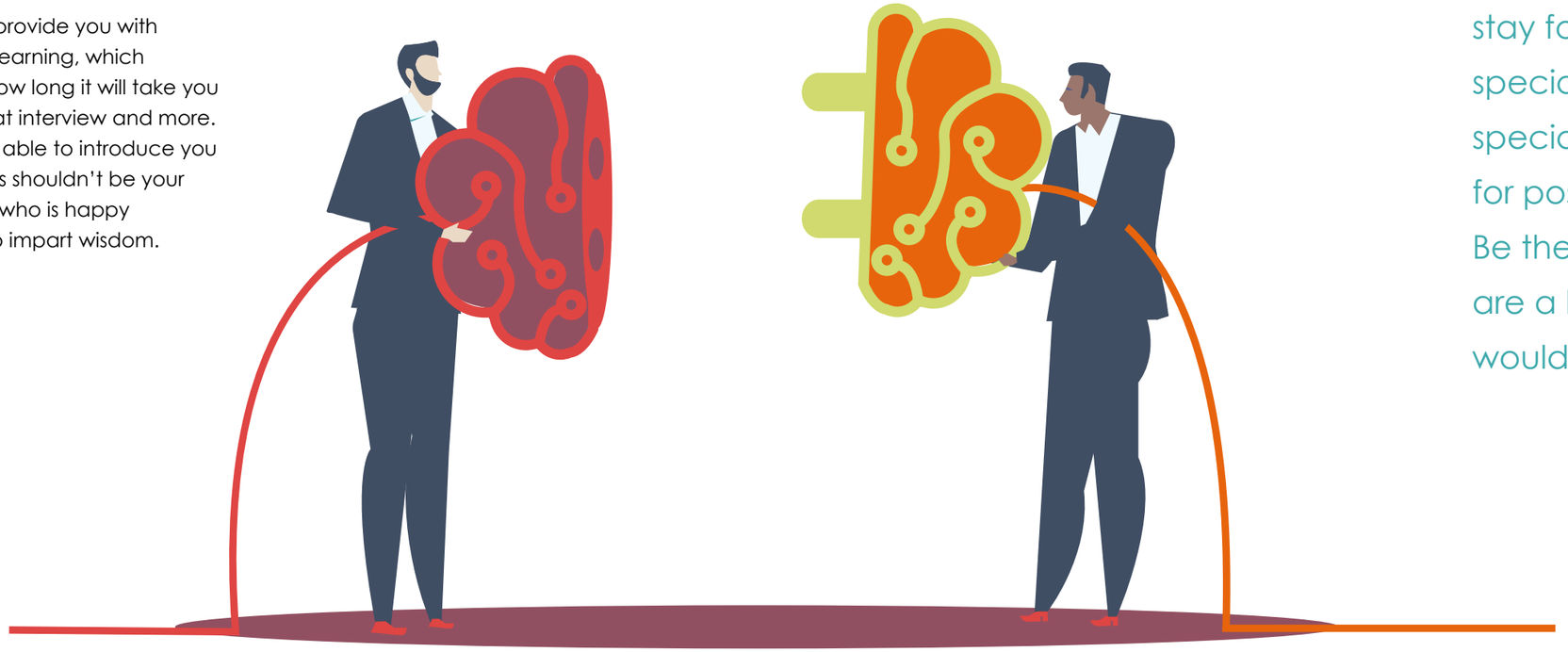
It's difficult to begin a career in cyber security if you are relying on the internet to help you. Training companies and certification providers with the biggest advertising and marketing budgets - those who will appear at the top of any search engine - are not necessarily the correct ones for you.

Chasing certifications - especially when you have no proof they will help you find a job - can be an expensive waste of time. It's important therefore to find a mentor who is already in the field of cyber you wish to enter.

This person should be able to provide you with objective opinions about self-learning, which practical skills you will need, how long it will take you to find a role, how to present at interview and more. They may - if you're lucky - be able to introduce you to potential employers, but this shouldn't be your priority. Instead find someone who is happy to support you, to listen and to impart wisdom.

Taking the time to find the correct mentor for you can be invaluable in gaining the correct, impartial advice you need.

Where do you find someone like this? Join membership organisations such as CIISec, SASIG and the UK Cyber Security Council (if you don't know what these organisations are, here's a timely reminder that curiosity, self-learning and awareness of the industry are crucial in getting a job - so now's the time to start researching). Engage with them wherever possible. Attend security shows and - instead of visiting the trade stands where you will only talk to sales people - attend the talks held by industry experts. Create a LinkedIn profile (more of that later) and become a voice people want to hear. Think "What can I do for you?" Not "What can you do for me?". The more you offer insight and curiosity to someone in this industry, the more likely you will build a rapport with them.



Once you have found someone whose guidance you trust - ask their advice on every step you take. Don't commit to an expensive course or certification without making sure it's right for you. And remember to stay focussed on your chosen specialism - don't be swayed by special offers, or answer job ads for positions you're not suited to. Be the person that - when you are a leader in this field - you would want to employ.

3. Build your skills.

So you know which area you wish to work in, and you have found a few people whose advice and guidance you are following. What next?

This depends on the specialism you have chosen, but in the majority of cases will require you gaining practical experience on top of any academic, formal education you may have received.

It's an uncomfortable truth that many UK-created cyber security qualifications, even Masters degrees from NCSC-certified universities, do not prepare students for a real-world job. Employers rarely rely on formal education to tell them a student is worth employing - so, while formal degrees have their place and you should be proud if you have one - it's time to accept that a career in cyber security will not fall into your lap just because you have been to university.

Why is this? Because the world of Information Technology is changing all the time - think of how quickly cloud, AI and quantum computing have entered our world. A formal syllabus simply can't keep up. Threats evolve at the same rate, if not even faster, than IT solutions - meaning that theoretical learning can only ever take a high-level view of what is happening. Once you understand that, you can begin to build a skill set that matches your chosen specialism, to add to what you learnt at university.

Technical cyber security - the 'offensive' (red) side of cyber which includes penetration testing, hacking, red teaming and incident response - will require practical skills which you will need to be able to demonstrate to a potential employer. If you have determined that you are more interested in a career in defensive cyber (the 'blue' side) you may wish to research areas such as ethics, law and governance. There will always be a crossover of skills regardless of which area you choose to specialise in - ***at the very minimum you should make sure you are able to demonstrate the skills on the following page:***

1. Fundamental technical skills

You should be comfortable demonstrating your practical experience of:

- **Network configuration and management**
- **Firewall installation**
- **Programming - see below**
- **Administration of various operating systems**

2. Programming

Programming and scripting languages are considered core competencies for cyber security professionals. The following are examples of languages you should consider learning:

- **Python**
- **SQL**
- **Java**
- **JavaScript**

This isn't a definitive list - ask your mentor what you should learn, and be prepared to self-learn different languages and programmes as they appear - this is a career-long journey.

3. Analytical skills

Risk management and data management are both ongoing tasks that require regular monitoring and analysis. You need to be able to show you can undertake a basic risk assessment as well as display an understanding of which tools can be used to manage and protect data.

4. Troubleshooting

Inevitably, when working in cyber security problems and issues will arise, often alarmingly quickly. You will need to be able to demonstrate quick thinking, logic, problem solving and reasoning - think about other areas of your life where you need these skills and include them in your CV.

5. Adaptability

How can you demonstrate that you are adaptable? What challenges have you faced in life where you have needed to change direction, think on your feet and leave things behind that are no longer helpful? Working in cyber means constantly having to stay one step ahead of the threat actors - which means being able to adapt very quickly.

6. Communication skills

It cannot be stated strongly enough that good communication skills - both written and verbal - are essential when working in cyber. You will often be asked to discuss risk, threat, vulnerabilities and technical terms with people who don't have the same background as you - an ability to write and speak well is one of the main 'soft' skills an employer will be looking for.

4. Manage your profile

Essentially, your personal profile consists of three elements:

- **Your CV**
- **Your LinkedIn and social media profiles**
- **Your covering letter**

Getting your CV seen

If you send out the same CV and the same letter to everyone you contact, expect to fail. See each role as a unique opportunity to showcase your skills and experience, and ensure you tailor your application to the specific role.

Don't get lazy - it's very easy to spot. Create a different CV for EVERY job, constantly add to it as you build experience and skills, and remember - it's not what they can do for you, it's what you can do for them. Research the company - have they been in the news recently, won an award or announced a new client? What software or certification body do they endorse? Who is on the team and what skills do they possess? Be the person who researches every aspect of a company and its employees and you will be steps ahead of other candidates. Don't rely on recruitment agencies to give you this information - do it for yourself.

Something to keep in mind: many companies use ATS software to rank CVs, meaning a computer will look for keywords within your application and make sure they match the job spec; if they don't, your CV won't even be seen by a human, let alone be read by one. Make sure you extract the keywords from job specs and add them to your covering letter and CV.

Don't worry if you don't have all the skills and requirements a job posting is asking for; with the current skills shortages recruiters are under pressure to find candidates and will create an unrealistic set of requirements, which they know they won't find in one individual, especially for entry level roles. If you can see there is a natural fit between you and the job - apply and do your best.

Be concise, use keywords, make the CV about you and you alone, use quantifiable metrics where possible and ensure that you have listed your 'softer' skills such as writing and communicating as well as any practical or technical experience.

If you are serious about getting a job in cyber security, you need to get serious about LinkedIn. There are many videos and articles available to help you build a profile and a follower count which will help you in your job search - ask your mentor for advice, and remember again the adage "What can I do for you?"

People like LinkedIn because they perceive it as adding value and knowledge to their working day. Just because you are starting out on your career doesn't mean you can't be a helpful and valuable member of the LinkedIn cyber community.

You can share resources, source articles, include links to white papers and offer opinions on other people's posts - all this establishes you as an independent thinker who engages with the cyber community and isn't afraid of contributing. Your profile will definitely be taken into consideration by potential employers so it's a valuable selling tool - but don't just use it as a job hunting platform.

Start to reach out to recruitment agencies and hiring managers, who will be able to help further with job descriptions, key words etc. However always remember that their agenda (to make money from placing you in a role) may not always mean they have your best interests at heart. Stay objective.

Here are some tips to help you build your profile:

- **Aim to post original content a couple of times a week - this can be reposted, or shared from a news site. Sign up for relevant emails from companies in your field and share their content - it establishes you as an expert.**
- **Set up Google Alerts for relevant phrases - for example new stories about breaches or cyber attacks - and share the stories as they happen.**
- **Follow industry leaders and engage on their posts, follow their followers and aim to be consistently growing your follower count.**

Make sure that your personal profile consists of:

- **A descriptive headline and eye-catching but professional imagery.**
- **A concise and engaging 'about' section - include all practical and life skills; remember prospective employers will see this.**
- **Include up to date experience, and remember to add relevant keywords. Testimonials are important, even if they are from jobs outside of cyber - your 'soft' skills need to be demonstrated here too.**

Hopefully you will have found this brochure helpful - read on to find out more about The Cyber Scheme.

Established in 2013, The Cyber Scheme is a leading assessment body and an NCSC Certified Delivery Partner for technical training and exams. The exams and training we provide are simply the best available; security testers who pass our assessments demonstrate competence and skill at the highest level defined by the UK's National Technical Authority for Cyber Security (NCSC).

The Cyber Scheme Foundation Level (CSFL) training course is designed for anyone wishing to begin a career in technical cyber security. It has been specifically developed to measure the competence of a junior and/or graduate cyber security professional looking for an entry level role.

In person training – the sure route to success.

To support the assessment, The Cyber Scheme has developed a comprehensive training course which will highlight and enhance the skills and knowledge required in order to be successful in the exam. The course takes place over two and a half days from a purpose built assessment centre in Cheltenham – following The Cyber Scheme's belief that in-person training is of a much higher level, is much more bespoke and is much more effective than anything provided online or remotely.

Candidates are immersed in the world of cyber security with practical hands-on exercises and expert tuition from a Cyber Scheme Instructor. They will learn about Linux systems, Windows systems, how to script in bash and in python. Also taught are the fundamentals of computer networking, web application technologies and vulnerability scanning, as well as the laws and ethics associated with security testing. This training will give candidates the essential skills of an ethical hacker at junior level.

Want to know more? See the complete syllabus here.