Cyber Security Careers Guide

for University Students

Join cyber first.

CREST®

inspired-careers
success is helping others achieve

"There are incredible individuals striving to keep the services we rely on safe from cyber criminals, but there simply are not enough of them"

Ian Glover, president of CREST

Introduction

It has never been easy for students to find their ideal job, but this year the task got a little harder with the news that graduate job vacancies have fallen for the first time in four years. Available jobs fell 8% year-on-year, according to the Association of Graduate Recruiters Annual Survey[1]. But there are still thousands of posts open to university leavers, and the good news is that one sector is bucking the trend – IT & telecoms is the only industry where the number of graduate vacancies is still rising...and one particularly strong area of IT recruitment is in cyber security.

Cyber security has become more and more prominent, moving from a back-office 'techie' activity to an industry that is at the heart of Britain's business success and its protection from major online criminals and terrorists. Recognising this, the Government has invested almost £900 million in a National Cyber Security Strategy to ensure government, businesses, law enforcement and UK citizens have the right skills and knowledge to combat cyber attacks[2]. But the threat remains severe: according to HM Government, 90% of large organisations and 74% of small businesses suffered a security breach last year[3].

All this has triggered a massive surge in demand for people with information security skills, and a growing shortage of such individuals. Worldwide there will be a shortfall of 1.5 million information security professionals by 2020[4] says ISC[2]. Such scarcity has driven up the value of cyber security experts, making this a highly attractive and lucrative career for UK university graduates.

This guide gives you the information you need to decide whether the cyber security profession is right for you, and how to get into it.

Whether your degree is in cyber security, IT, a 'STEM' or completely other discipline, you can thrive in information security. Employers are looking for people who are quick thinkers, strong communicators and have an inquisitive and analytical mind. So if that is you, why not consider one of the most dynamic industries in the world, where you would be making a real difference, and getting well paid for doing so?

This guide gives an overview of the cyber industry, the nature of the work involved and the threats you would be dealing with. We show the salary you can expect; the skills and qualifications you need to get into the profession; and the different routes you can take, including degree, masters and conversion courses, work placements and Internships.

The guide shows where to look for jobs and how to apply, with advice on building your CV, interview techniques, networking and other non-academic activities that can help get you noticed by employers. Finally, there is wide range of further sources of information.

Turn the page to find out more...

Sources:

[1]www.agr.org.uk/write/Documents/AGR_graduate_vacancies_press_release.pdf

[2]www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-the-final-annual-report

[3]www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html

[4]Frost & Sullivan/ISC(2) 2015 Global Information Security Workforce Study –
 http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html

Why join the cyber security industry?

There are many reasons to consider a career in information security. Here are a few...

Something for everyone

There is huge demand for cyber security professionals in the UK. The Science and Technology Committee of MPs has called it a 'digital skills crisis' – reporting that the commercial operations of 93% of tech companies are being affected by the skills gap, creating a growing need for cyber security and other skills[1].

So what does the work involve? The core cyber roles are security consulting (advising organisations on their security strategy), engineering (designing and creating safe IT systems) and operational security (monitoring computers for signs of attack, analysing where security breaches have occurred, and strengthening systems against such breaches). The operational roles range widely, from front-line defenders who protect data and networks from unauthorised access, to penetration testers who explore systems to expose security weaknesses, through to forensics investigators who analyse how cybercrimes or data breaches have occurred[2].

But while technology skills are very valuable when it comes to working in cyber security, this is not just a career for 'geeks'. The key attributes you need to work across the industry are to have an interest in IT; to be a quick thinker and strong communicator; and to have an inquisitive and analytical mind, with the ability to think outside of the box, because the work often involves problem solving and out-thinking attackers.

The industry needs a range of skills, so whatever your capabilities and interests, there could be a role available for you. In addition to technology-based careers, other options include:

– Business and IT security risk analysis

– Cyber security cultural change managers

– Digital forensics analysts

– Legal and regulatory compliance specialists

– Cyber security policy developers

– Cyber security project management

– Specialist recruitment

– Cyber security and vulnerability research

– Cyber risk management

– Threat intelligence officers

– Cyber security training and education

All these different career pathways can lead to senior technical and management positions within the industry. Even among the technical security roles, there is a huge choice. Inspired Careers (http://www.inspiredcareers.org) outlines dozens of different roles, from penetration testing and cyber incident response to network monitoring and security product design. To show what is involved in this industry, Inspired Careers' website features 'Day in the Life' films where a wide range of professionals explain their job roles.

– Visit http://www.inspiredcareers.org to see cyber security professionals talk about exactly what they do, and how they got into the industry

Sources:

[1]http://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf
[2]See Inspired Careers (http://www.inspiredcareers.org) and TARGETjobs (https://targetjobs.co.uk/) for more detailed information on job roles

Money makes
the world go round

The world has woken up to the need for information security professionals, with reports in the news almost every week of new cyber-attacks. Faced with this online threat, business and government are looking for experts who can protect their systems from cyber criminals – and they are willing to pay high salaries and provide continuing training and development.

That means there are great opportunities and benefits for anyone starting a career in cyber security:

– Salaries in information security are among the fastest growing in the UK – rising at an average 14% a year[1].

– For senior security professionals, average earnings are just under £100,000 a year[2].

– Your earnings are based on merit, not your sex, age or ethnicity.

What about at the beginning of your cyber career? The starting salary for a graduate working in information security is typically £20,000-£25,000 a year, according to the Prospects guide[3]. After a year's experience, you can earn up to £35,000; and after five years, working in more senior roles, you can command £40,000-£60,000 a year. IT Jobs Watch confirms that the median salary for cyber security professionals is £60,000[4].

Then there is another bonus – literally. Harvey Nash statistics show that the majority of IT (not just cyber security) leaders receive extra benefits worth 10-30% of their base salary, such as a car, incentive plans, shares and equity. One in 25 IT leaders get bonuses that exceed their base salary[5].

Of course a career in cyber security is not just about the money, but it helps.

"The growing importance of information security to organisational growth, and growing awareness by senior business leaders as to the value of exceptional information security talent, is helping to define a positive opportunity for information security skills remuneration"

Harvey Nash

Sources:

[1]Robert Walters annual Global Salary Survey – https://www.robertwalters.co.uk/salarysurvey.html

[2]Harvey Nash & PGI Cyber Security Survey 2016 – http://www.harveynash.com/group/mediacentre/2016/01/almost_half_of_boards_lack_real_understanding_of_cyber_threat_harvey_nash_pgi_cyber_security_survey/index.asp

[3]https://www.prospects.ac.uk/job-profiles/information-security-specialist

[4]http://www.itjobswatch.co.uk/jobs/uk/cyber%20security.do

[5]Harvey Nash and KPMG 2016 CIO Survey – http://www.harveynash.com/group/mediacentre/HarveyNashKPMG_CIOSurvey2016.pdf

Be part of a dynamic industry

It is clear from films and TV that cyber security experts are becoming high-profile and highly valued. From CSI: Cyber to James Bond's sidekick 'Q', cyber security is portrayed as an exciting, innovative and cutting-edge career.

This glamorous film image is not that far from real life! Governments, businesses and consumers know that cyber-crime is one of the fastest growing and biggest threats they face. The Office of National Statistics estimates there were over 2 million victims of cyber-crime in the UK in 2015[1]. And it's predicted that online crime will cost businesses worldwide as much as £1.5 trillion a year by 2019[2].

Every day there are attacks, from major corporate hacks to the theft of people's credit cards and personal data. In 2016, cyber-attack victims have ranged from the UK rail network[3] to the campaign team behind Hillary Clinton's bid to become US President[4], while over 100 million 02, Twitter, Yahoo, Hotmail and Gmail customers have seen their private data leaked online[5].

As a result of such crimes, cyber security experts are among the most prized professionals worldwide. What is more, the threat is constantly changing, which means you will always be learning and developing new skills and facing new challenges.

The cyber security industry has to constantly evolve so that it can protect business and individuals from new threats from all the latest technologies.

Without a dynamic cyber security industry the benefits that can be derived from new technology cannot be realised. Jobs that had not even been thought about five years ago are now established with great opportunities and careers.

There is nothing dull or repetitive about a career in cyber security!

Sources:

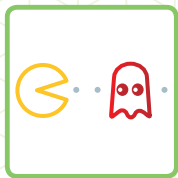[1]http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

[2]Juniper Research, 'The Future of Cybercrime & Security'– http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[3]http://www.telegraph.co.uk/technology/2016/07/12/uk-rail-network-hit-by-multiple-cyber-attacks-last-year/

[4]https://www.theguardian.com/us-news/2016/jul/29/hillary-clinton-computer-network-hacked-democrats-fbi

[5]http://www.bbc.co.uk/news/technology-36764548: https://www.identityforce.com/blog/2016-data-breaches; http://www.wsj.com/articles/twitter-millions-of-accounts-at-risk-of-breach-1465510623

Working for the greater good

Cyber-crime is both global and personal. UK companies have to defend against hundreds of thousands of cyber-attacks every day, and in some cases we have seen attack numbers increase by 1,000% in just 18 months[1].

But it is not just big business under threat: it could be someone you know. Take the case of the single mother of two from County Down in Northern Ireland who was robbed of nearly £77,000 in an email 'phishing' scam. She is just one of many individuals who get targeted by cyber criminals on a daily basis.

You could make a real difference by helping to keep people like this safe. Across the UK, the National Crime Agency, police forces, company security teams and special initiatives like Action Fraud, Cyber Streetwise and GetSafeOnline are all fighting this menace – but they need more help.

If you want the satisfaction of doing a rewarding job and if you want to make a real difference... join the cyber security community. There are great opportunities waiting for you with the government and the police, as well as working for the private sector.

"We need to tackle the skills shortage head-on and encourage the very best people to choose cyber security as a career path – an extremely challenging, exciting and rewarding one"

Ian Glover, president of CREST

Sources:

[1]The Times – http://www.thetimes.co.uk/tto/business/davos/article4670343.ece

Everybody wants you!

The UK is a cyber world-leader, with a growing reputation for being at the forefront of industry, research, innovation and fighting international cyber-crime. More than 40,000 people already work in the UK information security industry and demand for cyber skills is growing fast in every type of company and government department[1].

Regardless of size or type of organisation, they all need security experts to protect their sensitive data and customer information. Which means that if there is an industry you would love to work in – whether it be sports or fashion, media or the emergency services, finance or retail – cyber skills could be your route in to that sector.

And this situation isn't going to change any time soon. With three-quarters of IT decision makers reporting a cyber security talent shortage across the UK[2], this will stay an exciting and rewarding in-demand career – across every industry – for years to come.

"The cost of cyber-crime to the UK economy is billions of pounds per annum – and growing. There are millions of individual victims, many thousands of corporate victims and correspondingly substantial losses. Cyber-crime activity is a major and growing threat"

UK National Crime Agency[3]

Sources:

[1]Cabinet Office – https://www.gov.uk/government/news/new-pathways-for-the-uks-future-cyber-security-experts

[2]http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

[3]http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

The world is your oyster

The UK cyber security industry contributes over £17 billion to the UK economy[1]. Tens of thousands of home-grown experts are working to protect UK businesses, government agencies and consumers.

On a global scale, the rise in online crime is outpacing the supply of cyber defenders – and the UK's reputation for security skills means overseas buyers are beating a path to our door. Exports of UK cyber products and services are growing by over 15% a year[2]. That means there are plenty of opportunities for UK cyber professionals to work overseas; and information security's highly transferable skills mean you can move anywhere in the world.
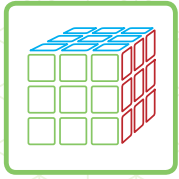
So if you want to experience life and work in other countries, a career in cyber security might just be your passport to success, opening the door to exciting international career opportunities from Africa, Asia and Australia, to mainland Europe, Canada and the USA.

Sources:

[1]Cabinet Office – https://www.gov.uk/government/speeches/governments-role-in-supporting-the-cyber-security-sector-matt-hancock-speech

[2]UK Trade and Investment –
https://www.gov.uk/government/statistics/uk-defence-and-security-export-figures-2013 and https://www.gov.uk/government/statistics/uk-defence-and-security-export-figures-2014

Cracking cyber security problems is the ultimate challenge

Is information security the right job for you?

The ideal career is one where you are valued, well-paid, enjoy yourself, are continually challenged, make a difference, and get great job satisfaction while you are doing it. Cyber security ticks every box. Not only is it in-demand, but if you like problem solving you will spend time doing what you do best, overcoming new challenges on a daily basis.

So how do you know if cyber security will suit you, and whether you have the right skills and aptitude to succeed in this profession? One good way is to try out the free cyber games and competitions, such as Cyphinx, provided by the Cyber Security Challenge.

Cyber Security Challenge UK is the first virtual environment designed solely to find and nurture cyber talent. This 3D world looks like a skyscraper where budding cyber security professionals play games and competitions, allowing you to test, improve and demonstrate your cyber skills to other participants, and to potential employers.

Some games link back to the Challenge's annual programme, which culminates in a 'Masterclass Grand Final' every November. Others are just for fun. The games blend traditional cyber security ciphers, code-breaking puzzles and contemporary gaming ideas, to reflect the real-world skills cyber professionals need to demonstrate. Visitors can try their hand at stopping the bad guy 'insider' causing havoc in an office network, and performing digital forensics on suspect files.

Anyone can use Cyphinx, from students to professionals already in the cyber industry, whatever their skill level or age. Cyphinx also offers more than gameplay. Its lobby area acts as a virtual meeting hub for UK cyber talent and employers, where they can share ideas, showcase their performance and discuss opportunities.

Every element of progress in every game/competition is recorded in the visitor's profile which is available (should they wish it) to other visitors and sponsors – many of whom may be potential employers. This way, organisations can identify talent with the specific skills for roles they need to fill; and visitors can select and play games that showcase the talents for which they want to be assessed as potential employees.

Cyphinx sponsors include prominent security companies such as the SANS Institute, BT, Clearswift, GCHQ, QinetiQ, Northrup Grumman, BAE Systems, Airbus, Raytheon and PwC.

It doesn't matter if you are highly technically competent, or brand new to the world of cyber – by getting involved with Cyber Security Challenge, you might just find you have a talent that leads to a rewarding career.

Visit https://cybersecuritychallenge.org.uk

How to get into the cyber security industry

With the huge and growing need for cyber security professionals in the UK and worldwide, there are many available roles to choose from and many routes to a successful cyber security career. So which is best for you?

Key skills needed

As described earlier, the core roles in information security include advising organisations on their security strategy; designing safe IT systems; monitoring networks for attacks and analysing where security breaches have occurred. There are also numerous 'non-techie' roles, such as business and risk analysis and management, regulatory compliance, policy making, threat intelligence, research and training.

But across the industry, the key attributes employers are looking for are people who have an interest in IT; are quick thinking, inquisitive and analytical; are good at problem solving and can think outside of the box. So if this is you, what formal qualifications do you need?

Qualifications required

Working in information security clearly suits graduates with a degree in cyber security, computer science or a related STEM (science, technology, engineering and maths) subject. According to the Prospects website, approximately half of information security specialists have an undergraduate degree, with the most common degree subject being IT.

But graduates from other backgrounds such as business studies and others can thrive in this profession too if they have the right attributes described above. Check out the job sites listed in the 'Where to find a job' section below for different employers' requirements.

In addition, there are a number of other actions you can take during and after your degree course to improve your chances of a cyber security career.

Masters degrees

Postgraduate study can be a good way to develop your information security knowledge and skills, and stand out to potential employers. A number of Masters degrees in cyber and systems security, cyber defence, digital forensics and the like are available.

These include a range of courses either fully or provisionally certified by the Government Communications Headquarters (GCHQ). As of September 2016, GCHQ had validated 18 Masters programmes at 15 universities – Birmingham, Cranfield, Edinburgh Napier, Kent, Lancaster, Oxford, Queen's University Belfast, Royal Holloway London, University of London International Academy, Southampton, South Wales, Surrey, University College London, Warwick and York. Details are available from each institution.

The Government has also set up two Cyber Security Centres for Doctoral Training (CDTs) at Oxford and Royal Holloway Universities, which offer doctoral-level training in cyber security skills. The Oxford CDT focuses on emerging technology themes and cyber security challenges such as the security of 'big data', cyber-physical security, effective systems verification and assurance, and real-time security. Royal Holloway focuses on problems faced by businesses and government such as design of cryptographic algorithms and protocols, and the detection and analysis of malware. A full list of Masters-level cyber courses is available via http://search.ucas.com/.

Conversions

One-year conversion courses are a good way for graduates to gain the specific knowledge they need to work in cyber security and improve their employment prospects. Some courses are designed for those with a degree in a STEM or other 'cognitive' field; others welcome graduates from a wide range of backgrounds. Examples of these include Plymouth University's MSc Computer Science (Conversion) course, which is aimed at graduates with a first degree in a non-computing related discipline; and Southampton Solent University's MSc in Cyber Security Engineering conversion course, designed for students from a range of academic backgrounds who have an interest in tackling cyber-crime and managing security systems. The choice of postgraduate options can be found by searching online for 'conversion to cyber security courses'.

Cyber Security Challenge UK has also launched the UK's first Extended Project Qualification (EPQ), a distance-learning course available to any individual, whether they are a current student or not, looking to get a foot in the door for a cyber security career. The EPQ is a level-three qualification, the equivalent to an AS Level, utilising the Challenge's Play-On-Demand gaming system.

See more at https://www.cybersecuritychallenge.org.uk/education/epq

Graduates can also work in a related IT job, then migrate into the information security profession. Cyber Security Challenge points out that many security disciplines are specialisms that can be learnt or progressed into – for example, a networking professional might move to network security or forensics, an application developer could progress to application security testing, and a systems administrator could develop forensics skills.

Another option is 'MOOCs' (massive, open online courses) which can help learners improve their cyber security knowledge and awareness by introducing them to basic cyber security concepts. These can be found via an online search.

CREST's YouTube Channel at - www.youtube.com/CRESTadvocate also includes useful content for learning about cyber security and what it is like working in cyber security.

Internships, Work Placements and Apprenticeships

CREST, the cyber security training and standards organisation, offers a Student Membership scheme. As part of this, CREST circulates the CVs of students available for internships or work placements to representatives from its member companies.

See more at http://www.crest-approved.org/

Internships or work placements are a useful way for graduates to gain practical, real-world experience in cyber security, and find out whether it is the right profession for you. They enable both the intern and employer to get to know each other, and may be a route to a permanent job with that organisation. Many cyber companies offer students and recent graduates summer or year-long (i.e. 2-12 months) internships or typically shorter work placements where the intern receives supervised practical training within the company. This may be paid or unpaid work.

Large employers typically advertise their internships and placements widely, including via their own websites and TARGETjobs (https://targetjobs.co.uk/). With smaller employers, TARGETjobs recommends that you hunt around their sites, make speculative applications, or look for vacancies via http://www.step.org.uk/; this site specialises in organising paid student work placements and graduate internships.

For graduates unable to find a suitable internship or work placement, TARGETjobs suggests approaching local companies, or contacts in your family and friends network, to set up 'work shadowing'.

The Cyber Security Challenge also advertises paid internships via https://cybersecuritychallenge.org.uk/careers/internship/.

Backed by the Government, Cyber Security Challenge is also running a series of 'cyber camps' to help graduates and students bridge into cyber careers. The cyber camps, delivered in association with universities, offer participants hands-on experience of cyber security over several days, and the opportunity to gain an industry-recognised foundation qualification in the subject.

See more at https://cybersecuritychallenge.org.uk/education/.

A number of employers also offer cyber security apprenticeships and degree apprenticeships aimed at those with GCSEs and/or A 'Levels. In addition, Tech Partnership, a network of employers working to create skills for the UK's digital economy, offers a Graduate Trainee Scheme which is open to any recent graduate in the East London area with a computer science or tech-related degree. This gives graduates paid work experience for 3-6 months, and the chance to show their potential in an IT role in London's 'Tech City'.

See more at https://www.thetechpartnership.com/techfuture/TechFuture-careers/graduate-trainee-scheme-students/

Non-academic activities

What else can you do to maximise your chances of as a successful career in the cyber profession? Here are some tips to show employers that you are keen and proactive:

– Participate in research activities and other events with CREST. Contact allie@crest-approved.org to join the mailing list for up to date information. Or follow @CRESTadvocate.

– Build up your knowledge. Follow security experts on Twitter. Attend industry conferences and events. Read cyber security publications, websites and blogs: specialist business, tech and security publications/sites include Ars Technica, BBC News Tech, Computer Weekly, The Economist, Harvard Business Review, InfoSecurity, New Scientist, The Register, SC Magazine and Wired.

– Network directly with cyber security professionals. Build your profile on LinkedIn and join security groups to find out more about the companies involved. Also, the IISP (Institute of Information Security Professionals) offers affiliate membership for people seeking a career in information security. No experience or qualifications are required to join. At the heart of the Institute is the IISP Skills Framework, which is widely accepted as the de facto standard for measuring competency of Information Security Professionals. Visit http://www.iisp.org/imis15/iisp/Member/Affiliate.aspx. Likewise (ISC)² offers free peer networking opportunities. To find out about joining an (ISC)² Chapter, visit https://www.isc2.org/chapters/default.aspx.

– Get some hands-on cyber skills by setting up your own hardware test environment, then trying out different attacks on the system, finding flaws and defending against them. But be aware that activities like penetration testing are illegal if carried out without permission. See http://www.sans.org/reading_room/whitepapers/threats/define-responsible-disclosure_932 for advice on this.

– Carry out volunteer work with a charity or similar organisation, who often need help securing their computer systems. For example http://cyberchampions.org/

– Send your CV directly to companies you are interested in working with.

Where to find a job

There are many specialist information security job sites and recruitment agencies. Prospects (https://www.prospects.ac.uk/), which provides advice on graduate jobs, postgraduate study, work experience and internships, recommends the following sites for job vacancies:

BCSrecruit – http://www.bcsrecruit.com/

Contractor UK – http://www.contractoruk.com/

CWJobs – http://www.cwjobs.co.uk/

CyberSecurity Jobsite – https://cybersecurityjobsite.com/

IT Jobs Watch – http://www.itjobswatch.co.uk/

Technojobs – https://www.technojobs.co.uk/

Applying for a job

So how do you maximise your chances of securing a cyber security job? When it comes to crafting a convincing covering letter, creating your technical CV and developing your Interview technique, there are many sources of advice. Among them, the National Careers Service has an online 'Get that Job' section with tips on building your CV and interview techniques (https://nationalcareersservice.direct.gov.uk/). Future Learn offers free online courses in how to write the perfect CV, application and online profile, and how to succeed at interviews. See https://www.futurelearn.com/courses/writing-applications and https://www.futurelearn.com/courses/interviews.

TARGETjobs offers downloadable templates of technical CVs and covering letters, and other 'job-hunting' tools. See https://targetjobs.co.uk/careers-advice.

Covering letter

- Be selective. The letter should be no longer than one side of A4. Pinpoint the top three or four attributes the employer seeks.

- Give examples of your academic, work and personal life to prove to recruiters that you have the skills, qualities and experience they're looking for.

- Thoroughly research the employer, its business strategy, culture, company values, products and services. Include the reasons why you have chosen this specific employer.

- Ask someone to check the letter for sense, style and grammatical mistakes.

Technical CV

- Always tailor your CV to each job you apply for.

- Capture the employer's attention with facts and information that show you meet the minimum requirements and have the right skills for the job.

- Include key technical skills (programming languages, platforms, systems, etc) that are relevant to the job. Indicate your level of ability and include brief information on how you have applied each skill.

- Don't exaggerate; and promote your soft skills.

Interview technique

- Review the job description carefully and make sure you fully understand what the employer does. Know the relevant skills needed for the role and the organisation's technical activities.

- You may be assessed through practical tests, design exercises, presentations or technical questions – or a combination of all four. Recruiters may ask you to comment on a range of scenarios or hypothetical situations of increasing complexity – or give you brain teasers – to assess your problem-solving skills. Candidates are often asked to work on a short design exercise or code analysis activity before the main interview begins.

- Many recruiters challenge candidates with problems that they're unlikely to have encountered before. The trick is to keep calm and give everything your best shot.

- Ask the interviewer if you think you need further information to complete a task. If you really don't know something, be honest.

- If you have put something on your CV, be prepared to answer questions on it. Never lie! Project work is a regular subject for discussion in graduate technical interviews, as recruiters can see how you have tackled a problem from beginning to end. Briefly explain what the project was about and the key objectives, then focus on the skills and techniques you used and how you overcame any difficulties.

Interview do's and don'ts

- Identify precisely what relevant experience and attributes you possess and make sure you communicate all these during the interview.

- Attempting to 'hijack' the interview will do you no favours; but this doesn't mean you have to be passive. Work within the framework they provide to sell your skills and experience.

- Don't be a know-all. Recruiters respect candidates who acknowledge gaps in their experience. If you need clarification about what you're being asked it's OK to say so, and to take a few moments' thinking time before answering a tricky question. If you don't know the answer to a question, admit this. Being caught out will do nothing for your self-esteem or your job prospects.

- Take all opportunities to ask about the role, in a positive way. Include the precise nature of the role, training and development, what previous recruits have progressed on to and your interviewers' own backgrounds.

- Treat your interviewers as human. A little 'polite-but-genuine' small talk at the beginning or end of the interview will mark you out a mature, thoughtful candidate who knows how to interact with others in a business context[1].

Sources:

[1]https://targetjobs.co.uk

Where next?

Here are sites and sources to help you find out more about starting a career in cyber security...

GCHQ's CyberFirst student bursary

A CyberFirst bursary is a programme of expert support that provides funding, skills and experience to launch yourself into one of the most exciting careers in technology. It covers three stages of your career:

University – during your study at university, you will receive a bursary of £4,000 per year, tax free.

Each Summer – we'll find you paid employment or training within government or industry - £250/week

After graduation – the opportunity to work for three years in cyber security roles in government or industry.

To Apply: **www.gchq-careers.co.uk**

CREST

http://www.crest-approved.org

CREST, the cyber security industry accreditation body, offers Student Memberships and circulates the CVs of students available for internships or work placements to its member companies. Also provides information on potential cyber careers paths through 'Day in the Life' filmed interviews with different people working in the information assurance industry.

Inspired Careers

http://www.inspiredcareers.org/

An interactive careers hub for people looking to enter cyber security from education or other industries. Outlines over 80 different cyber security roles, together with job and internship adverts, professional and academic courses, articles, white papers and social media advice. Features 'Day in the Life' films of people in cyber security.

Coursera

https://www.coursera.org/

Lists online courses from universities worldwide with a section on computer security and networks.

Cyber Security Challenge

https://cybersecuritychallenge.org.uk/

Helps graduates find cyber education and training opportunities and discover their hidden cyber talents. This site features Cyphinx, a 3D virtual world where budding security professionals can play games, and demonstrate their cyber skills to each other and potential employers. Has a good FAQs section with careers advice – see **https://www.cybersecuritychallenge.org.uk/careers/faqs/**. Also offers a graduate mentoring scheme and cyber camps. Advertises paid internships via **https://cybersecuritychallenge.org.uk/careers/internship/**. Runs the Extended Project Qualification (EPQ) distance-learning cyber qualification for people aiming for a cyber security career – **https://cybersecuritychallenge.org.uk/education/epq/**.

Future Learn

https://www.futurelearn.com/

Future Learn offers free online courses in writing CVs, job applications and interviewing. Also features a free, basic online 'Introduction to Cyber Security' course, developed by The Open University and certified by GCHQ. (A number of other free 'MOOCs' – Massive Open Online Courses – on cyber security are available by searching online.)

Girl Geeks

http://www.girlgeeks.uk/

Professional support community that helps connect female students talented in STEM (science, technology, engineering, maths) with businesses looking for them. Encourages women to make connections, share expertise and collaborate to encourage career development.

IISP

https://www.iisp.org/

The Institute of Information Security Professionals offers affiliate membership for people aspiring to an information security career.

(ISC)²

https://www.isc2.org/

Graduates can join an (ISC)² Chapter to network with cyber professionals.

National Careers Service

https://nationalcareersservice.direct.gov.uk/

Provides information, advice and guidance across England on learning, training and work opportunities. Helps users with careers decisions and planning and offers career-related tools.

Prospects

https://www.prospects.ac.uk/

Offers information and advice on careers, work experience and postgraduate courses. Features 400-plus cyber industry job profiles. Advice on writing CVs and cover letters. Job vacancies.

Step

http://www.step.org.uk/

This site specialises in organising paid student work placements and graduate internships.

TARGETjobs IT & Technology

https://targetjobs.co.uk/career-sectors/it-and-technology

This job search site and publication offers in-depth advice on graduate careers and professions, work experience, and training and internships. Provides tips for job hunters and downloadable templates for graduate CVs, applications and covering letters. Also data on IT sector employers such as key business areas, salary and benefits, number of vacancies.

Tech Future Girls

http://www.techfuturegirls.com/

Online club with challenges to help girls develop their tech skills.

Tech Partnership

https://www.thetechpartnership.com/

A network of employers aiming to create skills for the UK's digital economy. Provides information on tech degrees, courses and apprenticeships. Offers a London-based Graduate Trainee Scheme, giving graduates paid IT work experience for 3-6 months.

UCAS

http://search.ucas.com/

Lists Masters-level and other cyber courses.

CREST

HM Government

Join cyber first.

For more information please go to:
www.inspiredcareers.org