1 - Outline how the project works

Lesson 1 - Outline how the project works

CyberEPQ

Outline how the project works

"The CyberEPQ is the UK’s first and only Extended Project Qualification (EPQ) in Cyber Security. This unique Cyber Security qualification has been developed by a consortium of education and Cyber Security partners to help provide a starting point for anyone considering a career in Cyber Security; to go to university, start an apprenticeship or change career." (The CyberEPQ)

> What will I have to do
>
> ## What will I have to do?
>
> An investigation into a cyber security related topic of your choice.
>
> ### Outputs :
>
> - Production Log
>   - Forms for all the stages of the project
> - Gantt Chart / Planning documentation
> - Evaluation Table of Resources (or equivalent)
> - 5000-word essay
> - Filmed Presentation

> The Stages
>
> ## The Stages
>
> - Online Modules

- Initial idea brainstorming
- Production Log Stages
  - Record of Initial Planning (November)
  - Project Proposal - guidance and meetings (December)
  - Planning Review (January)
  - Mid-Project Review (February)
  - End of Project Review, Summary and Reflection (March)
- Presentation (March)
- Essay & Full Project Hand in (March)

Forming An Idea

What To Investigate

- Very rarely in life are we offered a completely free choice, so starting an Extended Project can be quite frightening.
- In reality though, it is likely that there will be some restrictions on what you can choose to do.
- How much choice do you really have?
- What format should your project take?
- The first thing to consider is which module or modules you are interested in from the CyberEPQ course and how you would like to develop them further.

Previous Years Project Titles

Previous Titles

2017-18

- Security Inside the Network: To what extent do employees impose a risk on an organisation’s cyber-security and how should these risks be minimalised?
- How did the attributes of the original Zeus malware enable it to dominate the internet banking malware industry and lead to an explosion of successful Trojan variants?
- How will Artificial Intelligence Change Cyber Security Practice now and in the Future?
- To what extent would Cyber Security be impacted were the UK government to ban end-to-end encryption.

- How can penetration testing and vulnerability assessment help to protect a business' assets?
- What impact does ransomware have on an organisation and what could be done to limit it?
- Why are cyber-attacks targeted at connected cars dangerous and what can be done to prevent them?
- How much of the vulnerabilities on a computer system is caused by human error in businesses and how can this be reduced?'
- Evaluate how successful are organisations who use Linux in protecting themselves from Malware?
- Critically assess if Cryptocurrencies should be banned in order to prevent Ransomware Attacks.
- How should the nuclear industry around the world produce effective solutions to tackle cyber threats?
- To what extent are Organisations putting their Cyber Security at risk and how can this be overcome?
- Examine how far business email compromise is the greatest Cyber Security threat to modern businesses.
- Explore the impact of whaling emails on large organisations and what can be done to rectify this.
- How and with what ease can cyber criminals access the data sent and received over public WiFi, and what measures can be taken to prevent this?
- To what extent does the Computer Misuse Act and other aspects modernise the Law Sector?
- Examine to what extent quantum computing can make public key cryptography more vulnerable and what are the possible solutions?
- Critically assess the impact that Biometrics has on society. CyberEPQ Project Titles of Cohort 2017-18
- Exploring the common features of phishing attacks against individuals, and how can this knowledge help to reduce the impact of phishing?
- Critically assess to what extent patching works and if patches should be openly released or forcibly applied?
- Wannacry; How hard is it to catch?
- Examine the similarities and differences of how ransomware may affect the individual and a company?
- Assessing the benefits and drawbacks of Penetration testing and how to make it more effective. 2 | P a g e CyberEPQ 2017-18 Project Titles
- To what extent can we protect ourselves from a Distributed Denial of Service Attack and possible solutions for the future.
- Examine the advantages and disadvantages of Vulnerability Penetration Testing within a system or a network?

- Assess how relevant anti-virus solutions are that run on computer systems against today’s ransomware attacks?
- Critically assess the contemporary significance of Computer Based Legislation and examine possible solutions.
- How safe is your device? Authentication, and the steps a user can take to ensure cyber security though authentication.
- An Investigation into the effectiveness of PIN, Android Lock Pattern and Fingerprint as Mobile Authentication Methods
- Data Breach Prevention and Response Best Practices - Lessons Learned from the Equifax Breach.
- Risks of Public Networks and how to solve them.
- To what extent does the insecurity of modern routers affect the security of connected devices and analyse how effective are possible solutions.
- Evaluate Worms and their effects on a business. CyberEPQ Project Titles of Cohort 2017-18
- Explore the advantages and disadvantages of Cybersecurity for businesses and how cyber risks may be reduced or eliminated?
- To what extent has digital forensics evolved and how effective are the tools available.
- Examining the failures of defending the WannaCry ransomware attack, and what were the lessons learned?
- Evaluating the future of security in Internet Of Things.
- To what extent do Darknet marketplaces and forums pose a threat to organisations?
- Evaluate the effectiveness of Autonomous Intrusion Detection Software used in Academia and what should be done to improve it.
- End to End Encryption, how can it be used successfully and should all communication be encrypted by default?
- Discuss how effective Future-proof as Current Standards of Encryption are to Quantum Computers.
- Critically evaluate which laws ethical hacking breaks and to what extent should be considered illegal?
- WannaCry: Inevitable or Negligence? Discuss.
- Ransomware: How easy is it to create and deploy?
- A critical comparison of PCI DSS and ISO/IEC 27001:2013 Standards

---

2018-19

- Explore whether being a victim to cybercrime is viewed by organisations and individuals as inevitable, but whether instead it should be seen as something that can be avoided with careful self-management.
- What might be the consequences of using hardware and software designed by foreign nations on UK national security and the privacy of the British public, and is the risk great enough to justify?
- An outline of the main tools available to pen testers, with examples of how they can be used.
- To what extent are end users the weakest links in Cyber Security?
- With the vulnerabilities associated with USB storage devices should they be banned outright in businesses?
- Why was the Stuxnet worm so successful?
- Have They Stopped Lock Bypassing and Acquisition of Data in Modern Smartphones?
- How are email users protected and what security is provided?
- With cybercrime at its peak, how have the security measures of the dark web allowed cybercriminals to thrive anonymously?
- How has the introduction of, and recent changes to, computer-related legislation affected the use of encryption in order to protect personal data?
- Are methods for preventing breaches more effective in the prevention of cybercrime, or are other methods more effective?
- With the theatre of cyber warfare advancing fast, just how safe are the highways in the skies?
- To what extent can the Internet of Things (IoT) vulnerabilities compromise other systems?
- How can an individual user or a company identify spear-phishing emails and protect themselves from spear phasing attacks?
- Artificial Intelligence in Cyber Security: Threat or Opportunity?
- What motivates black/grey/white hat hackers, how they develop to that role and how does the government/companies decrease the amount of black hat hacker?
- Should ‘grey hat’ hackers (Freelance cybersecurity professionals) be allowed a role in stopping attacks such as the WannaCry NHS breach?
- An evaluation of why humans are a weak link in the protection of networks.
- An Evaluation of Autonomous Automation in Terms of Security and Ethics.
- Malicious Crypto mining: What is this new form of malware, what extent can it damage and disrupt an organisation and what can be done to minimise these dangers?
- An Analysis instruction, detection systems and tools and how effective they are.
- The ethical considerations of Penetration Testing and the tools used.

- Evaluating Methods of Obtaining, Analysing and Preserving Digital Evidence Using Digital Forensics.
- To what extent should developers of devices that are a part of the “Internet of Things” (IoT) improve the security of their devices against attacks, and how does the security of these devices compare with regular computers?
- Can 'Deep Fakes' Change the World? Their creation and detection and the societal implications of their use.
- How worms can affect an educational institution.
- How effective pen-testing and vulnerability assessments are in identifying threats and protecting a business’s asset?
- Evaluate the different Methods of Network Intrusion and how to detect once unauthorized access is gained.
- The risk and reward of VPNs and PROXY servers.
- Most influential hacks in history and how Cyber-Security rose to meet them and protect from future hackers.
- What is the single best method black hat hackers use to attack modern businesses?
- An investigation into phishing – the reasons behind it, how much success phishers have, how we protect against it, and could we defend against it better.
- Exploring the effectiveness of Ransomware Hacks in modern enterprises, and how to circumvent them or deal with them successfully; highlighting the common weaknesses found in a company’s cyber-security.
- How the eagerness for the latest smart technology compromises the security of our society and the nuances of keeping our information private.
- Examine the advantages and disadvantages of vulnerability and penetration testing within a network, system and business.
- How have black hat hackers tried to break different encryption standards and where have they failed?
- Is Social Media really secure for you to put your personal data and information onto? and what are the biggest cyber threats that is being faced by social networking sites?
- Should the UK put electronic voting systems in place and if so, what measures should they ensure are in place to avoid any attacks on them?
- Does the efficiency of digital vote counting outweigh the potential risk of an accidental computer glitch or targeted cyber-attacks?
- How was Mirai able to dominate major sites such as Amazon and how was it stopped?
- How are professional organisations vulnerable to cyber theft and disruption?
- Quantum computing - the key to more vulnerabilities in public key cryptography?
- Do passwords protect or pass words to attackers to hack our systems?
- Challenges and Opportunities of Machine Learning in Cyber Security.

- Understanding the effects data breaches have on an organisation and the impact of counter–measures.

2019-20

- An Examination of whether Cybersecurity can prevent chaos focusing on Intrusion Detection and Analysis.
- Differences of limitations between Penetration Testing and Unethical Hackers.
- Exploring DDoS Attacks including SSL DDoS.
- Is Facebook doing enough to ensure that their users' data is secure?
- Evaluate some of the most damaging cyberattacks of all time and what organisations need to do to better protect themselves in the future?
- What is phishing and how has it evolved. What's coming next, and how can we stop it?
- An exploration of why ethical and unethical hackers are motivated, why it is so important to know how they operate, and how can agencies reduce the number of unethical hackers?
- What are some of the most damaging viruses and how could they have been prevented?
- To what extent do the vulnerabilities of computer hardware and architecture affect the performance and safety of a computer?
- Investigating vulnerabilities in public key cryptography caused by quantum computing and potential solutions.
- Can a computer ever be 100% secure?
- Identifying and assessing the biggest threats to a computer system.
- How computers have evolved since World War II and created the need for cyber security and why the need for cyber security is increasing.
- How is Artificial Intelligence going to affect cyber security?
- Why is digital encryption so important in our modern society?
- Where does our data Go-ogle? Investigating Google's data and collection usage.
- Ransomware: The top 5 most notable incidents, could they have been prevented and how could we prevent them in the future?
- How effective is the use of cryptography and encryption in securing personal data in the face of developing technological and political landscape?
- Can AI be of use in vulnerability identification?
- How robust are today's encryption standards and how will advancements in computing technology lead to changes in encryption?

- How Can Cyber Criminals Exploit Public Wi-Fi Hotspots and What Measures Can Be Taken to Minimise
  the Risk They Pose to the Public?
- Comparing the enforceability of cyber security legislation in developing countries.
- Does user anonymity on the dark web facilitate criminal behaviour and what measures can be taken
  to reduce such activities?
- Will we ever be able to stop cyber-attacks for good, and if so when?
- The Potential Impact of Quantum Computing on Current Encryption Methods. Evaluating the security
  impact due to current encryption methods being broken
- To what extent should medical establishments limit the use of technology whilst storing patient data?
  An analysis of the WannnaCry virus on the NHS, 2017
- What are the dangers of connected toys and who does this affect?
- What are the frontiers of Big Data and how will they affect society now and in the future?
- How Digital Forensics can aid solving criminal cases
- How best to keep yourself secure online on your smartphone?
- Is Digital Forensic Evidence now of greater importance than Traditional Forensic Evidence in Modern Policing and Crime?
- Are smart devices within our homes compromising our privacy, and if so, who is at fault and what are the possible consequences?
- How has the software industry responded to developments in software piracy and hacking, which responses have proven the most effective, and what does the industry need to do to prepare for the future?
- To what extent can VPNs protect a person's anonymity in a society that has cooperation spying on you and government mass spying programs?
- What is the importance of white box and black box penetration testing and how far do they ensure system security?
- Nowadays is human error the biggest threat to cybersecurity and how can this be prevented?
- What are the most effective steps that can be taken to secure a system, and can it ever truly be secure?
- How great is the risk surrounding the sale of USB Rubber Duckies to the public, which can be used for malicious purposes?
- Is it possible to recover potentially deleted data from secondary storage and what are the most effective methods of doing so? Does time have an impact on recovering the data?
- How have cyber-attacks and hacking methods developed over the years, which have been most effective and where should cyber security focus in the future?

- “Did the Sandworm group fully anticipate how destructive the release of notPetya would be?”
- Are free penetration testing tools viable?
- Can one safely use Public WiFi and if so, how?
- Do Botnets pose a major cybersecurity risk to businesses and people, and how available are they to someone with malicious intent?
- Should organisations consider ransomware a significant threat in 2020?
- Do the actions of employees create unnecessary vulnerabilities in a system?
- How Secure are Cryptocurrencies?
- How have security measures changed since major attacks have happened, and how can we be sure it won’t happen again?

2020-21

- When does government or international surveillance turn into an obsession over control, and how could this affect firms?
- The ethics listening AI, and how much of our data should others be allowed to have?
- Data collection in Windows 10: Why is it done, what do Microsoft and the media claim, and what does it mean for the average user?
- The impact of COVID19 on cybersecurity in a workplace. What are the implications of remote working and how security-aware are employees?
- An Investigation of the Impact of the EU’s Strategy for a Digital Future on Netizens’ Privacy vs Convenience and Big Tech.
- Security Through Obscurity and the Practicality of Esoteric Network Defence.
- Penetration testing and its role within the cyber security industry.
- Are Discord and WhatsApp in tune with Cyber Security or are they off-key, hidden spyware, in plain view?
- An Analysis of the Statistics of Global Hacking and an Examination of their Relationship with Global Geopolitics.
- Security as a Service : Outsourcing cyber security.
- Security in the Cloud: self and other in the enterprise cyber space.
- Should Encryption techniques such as End to End Encryption continue to be an industry standard for different applications and should companies be allowed to view the data being sent, received and stored?
- Is there a significant risk posed by the rise in remote working?
- How can the internet of things be misused (in particular - Botnets) and why is it proving so difficult to stop this misuse?
- Will we ever be able to stop Cyber attacks in the UK? If so, when?

- Investigating public-key cryptography, don't share the key!
- Dangers and Risks of SQL injection and how to prevent attack?
- How to stop DDoS?
- What are the ethics behind whistleblowing in Cybersecurity?
- How do people remain anonymous online?
- To what extent is ransomware the greatest cyber threat towards the functionality of hospitals?
- Is it possible to use the internet without being tracked?
- Identity Crisis: With identity theft on the increase, how can artificial intelligence make digital identities more robust?
- To what extent will the development of quantum computing impact modern cryptography?
- To what extent will quantum computing threaten today's crytographic infrastructure?
- To what extent should NATO nations allow other countries to provide internet services?
- Why is phishing one of the most widley used forms of cyber-attack in data breaches?
- Why are educational institutions vulnerable to malware attacks?
- How have developing countries adapted to the implementation of the Internet & how some dealt with being attacked from across the world?
- Analysis of how malware attacks have grown, how they are evolving, and how they will affect technology in the future.
- Has free streaming services killed off music piracy and what cyber security threats are there in downloading music legally and illegally?
- How does vulnerability assessment and penetration testing help in the security of self-driving cars?
- The differences and impacts of government funded and hacker run cybercrimes.
- How have cyber security practices developed to meet the challenges of cyber-attacks – in particular the Morris worm, ILOVEYOU worm and Stuxnet worm?
- Most effective methods of speeding up password cracking.
- How is Key Distribution Centre used? What industries use it? Can it be made more efficient in those industries who need it?
- In the future, could technology aid the government in creating a surveillance state?
- Is human psychology being neglected in the attempt to cybersecure smart cities?
- Can vulnerability assessments be implemented in smaller organisations/businesses and how can they impact these organisations?
- How has cyber warfare developed over history, what are some countries capabilities, and what does the future hold for cyber warfare?
- Do hacktivists cause more damage than good?

- What are the most effective ways of preventing against and responding to ransomware attacks?
- How do cybercriminals use ransomware to hold your computer as hostage? How I believe you can prevent ransomware attacks and comparing the different types of protection to decide on the best one.
- Open Networks: What are they and why do they exist?
- What does the use of quantum computers mean for the future of encryption systems? Is it possible to future proof encryption from quantum computing so that it will no longer pose a threat or is it a serious issue?
- To what extent is government surveillance good for a society?
- To what extent do organisations need to protect themselves from cybersecurity threats and what are the most effective methods of doing so?
- How big a threat is quantum computing to big business?
- Is Information Security taken seriously and what can be done to better people's data confidentiality and integrity on both an individual and organisational level?
- How viable is an offensive cyber strategy in protecting a nation's interests?
- What cyber-attacks and hacking methods have been most effective, how have they changed over time and what should be the focus for cyber Security in the future?
- The role of cryptocurrency in cybercrime: How cryptocurrency empowers cybercriminals.
- Is White Hat Hacking the Most Ethical Form of Hacking?
- How will Quantum Computers Impact the Security of Data Transmission?
- To What Extent are Neural Networks a Viable Defence Against Cyber Attacks?
- To what extent can the top 5 social engineering attacks be prevented?
- Should digital piracy be considered a serious, growing threat to cyber security and what are some ways to reduce the risk?
- How effectively can Artificial intelligence be implemented in penetration testing?
- What are the most important threats to voice assistants and how may they evolve in the future?
- An evaluation of human factors in cybersecurity with a particular focus on impulsivity.
- How does the SolarWinds hack and other attacks on networks and websites affect individuals and organisations and the importance of penetration testing and how to perform a penetration test to discover and patch any vulnerabilities?
- Why was the WannaCry Ransomware worm so successful and what are its future implications?
- Understanding the effects that WannaCry cyber-attacks have on different organisations and how these organisations are trying to prevent this from happening again.

- To what extent does hacking negatively impact the Quinary sector of the UK economy?
- How might the increasing development of Artificial Intelligence affect the world of cyber security?
- To what extent are employees the greatest threat to cyber security?

2021-22

- Digital footprint and our own information being used against us to manipulate our behaviour online and the violation that poses to GDPR and our own personal data while using the internet
- Why was the WannaCry Ransonware worm so successful and what are its future implications?
- To what extent does human behaviour compromise security with regards to financial safety?
- What factors influence the gender gap in the cyber security industry?
- Are Cryptocurrencies Really Anonymous?
- Evaluating privacy implications of Google's search engine monopoly
- Cloud Computing
- Non-proprietary software does more transparency increase security? Ways you could prevent another log4j situation
- What is scamming? Will we ever be able to stop scamming? How are we adapting to prevent it?
- How are socially engineered attacks initiated and how can schools mitigate these risks?
- What are quantum computers and how are they likely to influence data encryption and decryption?
- How secure is Bluetooth?
- An evaluation of penetration testing and its methods
- Analysis and evaluation of penetration testing
- How are digital forensic used and how useful are they in the criminal justice system?
- Evaluating appropriate policies for SMES to deal with the increasing cyber threat in the modern world
- What is SQL injection, how can cyber criminals exploit an organisation's backend vulnerabilities using injection attacks and what measures can be implemented to prevent and detect injection attacks?
- How can users of corporate systems reduce security risk? Is total security possible due to social engineering and deception? How can companies use these

social engineering techniques to identify weaknesses in their own systems and policies?

- What specialist hardware and software tools do Penetration Testers use and why?
- An internal penetration test of the Saffron Walden Baptist Church's Computer Networks to determine points of weakness from a malicious insider
- What can the Cambridge Analytica scandal tell us about the need for cybersecurity in the Metaverse?
- Is Black Box and White Box penetration testing an effective way of considering systems' security?
- Are online gaming communities sufficiently protected from modern cybercrime?
- Analysing and evaluating the use of digital forensics techniques in regard to homicide investigations
- What are the security methods behind Bitcoin, and can they be exploited?
- Do certificate signing and encryption offer sufficient protection in the age of Quantum Computing
- Why is the Computer Misuse Act of 1990 hypocritical from its design and is it fit for purpose today?
- How has the media coverage of the cyber world shaped public attitudes towards online security and how can we expect them to develop in the future?
- Can Artificial Intelligence replace humans in penetration testing in the Internet of Things?
- Is Cyber Piracy a severe issue in today's society and have the methods of preventing digital piracy attacks evolved to match the growing threat?
- Evaluating the implications for technology in cyber warfare given advancements in quantum computing
- To what extent should consumers be concerned about the cybersecurity risks posed by smart home devices and how might these concerns be mitigated?
- How the size of a company in the financial industry affects the success and impact of a cyber attack
- What is the future of homomorphic encryption with a focus on data analytics?
- How safe are cryptocurrencies, what implications are there for its adoption?
- What is a VPN, and should we use it?
- What is the public's opinion whether the GDPR are sufficient to protect the public against possible ethical problem with voice AI?
- How effective are passwords as a means of authentication, how can they be attacked and how can they be made more resilient to attack?
- Is your location and personal information safe while using a VPN?
- Why is incident response planning pivotal to the cyber security industry?
- What steps non-technical people will take to keep their personal data secure
- How reliable is digital forensics in determining a lawful outcome?

- WiFi security and Reliability - How at risk are we and what can we do?
- Phishing abd how not to get baited
- The History and Evolution of Cybercrime
- How has VR Technologies Impacted Social Engineering?
- The history of cyber forensics and how it has allowed the authorities to investigate crimes
- WannaCry - The ransomware that took down the NHS. Who was involved, how did they do it and why?
- To what extent are biometric systems secure from unauthorised access?
- To what extent is penetration testing effective against social engineering attacks?
- What risk does Cryptocurrency entail and is there a way to prevent it?
- When does Government or International Surveillance turn into an obsession over control and how does this affect firms?
- Remote Working
- Ethics of Whistleblowing in Cybersecurity
- To what extent is social engineering a driving force of Hacktivism?
- Were the US and UK right to cut Huawei out of future communication networks?
- How is MI5 effected by Cyberwar?
- How are CAPTCHAs using humans to train Artificial Intelligence?
- How can Artificial Intelligence be implemented in Digital Forensics for Data Analysis and Threat Recognition?
- The insecurity of the Internet of Things, a manufacturer's role in securing our technology-driven world
- How do schools keep children's data secure? How effectively are security information incidents managed and responded to, to ensure this security? An evaluation of strategies and tools

---

2022-23

- Security audit of a boat's Local Area Network
- Is electronic banking safe from cyber threats for users in the UK and what are key fundamental ways to mitigate its evolving threats?
- An examination of network security among home computers with pentesting case study
- The effectiveness of social engineering cyber-attacks within modern society
- How can the education sector maximise network security?
- Can you remain truly anonymous online, legally and ethically?
- How can business use cyber forensics to protect and ensure safety of its assets in the business?

- How has security evolved over time to help protect people from cyber-attacks?
- Is an individual's data privacy taken seriously in the UK and why do companies want as much of people's data as possible? Is this good for people and society?
- Ransomware attacks are currently the biggest threat to businesses
- How can we develop a cybersafe society?
- Can you be truly anonymous online?
- Evolution of ransomware with their mitigation and prevention techniques
- Is our information stored within the NHS safe from ransomware, and how can updated technical controls mitigate it?
- Is the Human Factor the leading cause of cybercrime?
- Should corporations fight back in a cybercrime cyber war?
- Exploring the impact of digital devices in Police (Forensic) investigations
- Security as a service; Outsourcing cybersecurity
- How is penetration testing used ethically by businesses?
- What is quantum computing and quantum encryption and what is the future of this technology?
- Discuss the different types of spyware and how can you protect a computer system from infection
- What is the most serious threat posed by IoT devices in the home?
- What prompted the Computer Misuse Act 1990 and how are we moving forward with it?
- Are the users the biggest vulnerability to the network and themselves?
- Are traditional authentication methods, such as passwords and PINs still viable or do we need to be moving quicker towards biometrics and other such authentication methods?
- Can advances in technology ever completely remove the human vulnerabilities from computer systems that require passwords?
- Menacing Trojan
- How feasible is it to mark identity online using VPNs?
- Phishing for data: An evaluation of whether phishing countermeasures do enough to protect users
- What techniques do scam call centres use to manipulate their victims into complying with their requests, and what techniques do ethical hackers use when trying to combat this?
- If an attacker has physical access to a system, are all hopes of security lost?
- How can systems and software evolve to combat information security attacks?
- Why people use cryptocurrency and how safe and anonymous is it?
- How does quantum computing affect the current crypto system, such as RSA encryption? How big will it affect banks and companies in the future?
- Safety of Encryption Algorithms: Their vulnerabilities and Preventative Measures

- What is brute-force attack, how it works and how to defend against it
- The impact of deepfake technology on my local community
- What is the scope and approach of cyber security in external audit today and how will this evolve in the future?
- Can algorithms be racist?
- The history and evolution of cybercrime in the UK 1970-2020
- How effective are passwords as a means of authentication, how can they be attacked and how can they be made more resilient to attack?
- A recipe for cyber security. Setting the foundations of cyber security
- What is the future of digital forensics?
- The prevalence and impact of call centre scams on individuals and organisations
- Why are digital forensics doing their job as they are and what events made them to this current state?
- Social media: Is it free or does it come at a price?
- What have been the biggest cyberattacks on DSPs and OESs in the past years, and how have they impacted the greater world?
- To what extent can continued education about password strength prevent the exploitation of the increase in use of RDP software?
- Do quantum computers pose a risk to online banking?
- An analysis into the intrusiveness of online surveillance
- To what extent does social media increase the vulnerability of a user and how can this be dealt with?
- The Legality and Ethicality of Penetration Testing within the UK
- Impact of malware on businesses, specifically hacking, that targets businesses containing large amounts of personal data
- Investigation into the usefulness of different penetration tools available to hackers in the UK
- Does video game hacking promote fraud?
- The effect of two quotients (Intelligence & Emotional) on cybercrime
- The threat of Quantum Computers on Encryption
- Privacy in the Digital Age: The challenges and tactics for protecting sensitive data in the NHS
- Deepfakes - How great is the threat?
- Are people more vulnerable to cyber security issues after the pandemic?
- How has social engineering grown to target vulnerable adults, particularly elders?
- Can a trade-off between security and performance be achieved in a computer network?
- Are cyber operations an effective weapon in interstate conflict?
- Is the admissibility of digital evidence determined in a just and consistent manner across all criminal cases in the UK?

- What impact can quantum computing have on encryption and how can we stay secure?
- What are the common types of cyber-attack that a small organisation may face and what countermeasures should be put in place in preparation?
- How can employees compromise your businesses cyber security and what prevention techniques could you use?
- Are there steps that can be taken to protect against cyberthreats in organisations with limited resources?
- How does a social engineer plan and deliver an attack?
- Cyber security arms race. How have cyber-attacks developed over time?
- Does white hat hacking make a difference in terms of future attack prevention?
- What makes an organisation the perfect target for a social engineering attack?
- Blockchain security and how the technology can be used in real life scenarios
- Is Government censorship ethical and/or practical?
- How does the war in Ukraine impact global security - have the focus, methods and techniques of state actors changed since the start of the war?
- How do client and pen tester set boundaries and how do they avoid accidently breaching them?
- How effective is AI at detecting rogue data packets on a network?
- How secure are RFID based security systems?
- How are networks commonly vulnerable to privilege escalation and how can these vulnerabilities be mitigated?
- Worms: Why are they made and how do they spread?
- Does behavioural-based malware detection have any negative effects on end users?
- Why does security culture vary in different organisations and nations?
- How does communication affect cyber security and how can the public be educated on how to stay safe online?
- Encryption and the ever-growing advancement in technology
- Malware in the UK Nuclear Sector: Assessing the threat
- How computers have evolved over time and how this has affected cybersecurity
- Does cryptocurrency influence cybercrime?
- Can mobile application policies shield police from a comprehensive digital forensic investigation?
- The consequences of social engineering in the modern world and the importance of prevention
- Data management in our modern world: exploring how companies and organisations use our data and the possibility of achieving complete privacy on the internet
- How does cryptography play a role in the security of online payments/transactions and cryptocurrencies?

- What are the consequences of the rapid evolution of artificial intelligence for the cyber security industry?
- Do the security vulnerabilities of blockchains prohibit the software from being used as a global standard?
- How can political and civilian organisations ensure protection from the threat of cyber warfare and cyber terrorism and the effects these attacks have on societies?
- Investigation into the dark web, technology that supports it, the nature of the activity that takes place and how it is managed by authorities
- AI is used in many cyber security firms and companies; how does this affect the way we view cyber security and how could it impact the future of cyber security?
- What was Stuxnet, how did it work, what were its effects and how can we learn from it?
- Why deepfakes are a major threat to the UK and what we need to do to limit this threat
- The Accenture Breach: Are third party cloud servers secure?
- How ethically sound is penetration testing?
- History and advancements of Trojan Horse RATs
- The repercussions of cyberattacks and the many effects of RockYou
- How did the Cryptography and Encryption of messages change from World War Two to the modern day?
- To what extent was the WannaCry ransomware attack pivotal in changing our approach to cyber security?
- Implementations of machine learning for DDoS attack prevention and anomaly detection in cyber security
- How TLS 1.3 provides its security
- Why artificial intelligence (AI) is key to protect schools from advanced cyber security attacks
- Project Doppelganger - A lesson in the consequences of trusting unencrypted RFID
- What type of threat poses the most risk to a US intelligence agency - internal or external?
- Smart home devices and cybersecurity: Evaluating the vulnerabilities in commonly used smart home devices, exploring the risks posed when they are exploited and measures to protect against these threats
- How can we manage cybersecurity in the dynamic world of cryptocurrencies?
- To what extent did the Stuxnet virus (2010) change the cybersecurity industry?
- What measures can be taken to hack-proof and strengthen the security of a website, and how can these be tested in a practical setting?
- What is phishing and social engineering?
- Will cybercrime ever stop and how will digital forensics help?

- How AI and Quantum Computing will change the world of cyber security
- How digital forensics are used to identify when encrypted messages that are sent across a network are intercepted and altered by hackers who gain access to the information illegally
- Has the relationship between digital forensics and the law evolved in the past 50 years? An investigation into how prosecution has changed with the introduction of digital forensics
- Does penetration testing have its limitations? An investigation into how pen testing secures networks and increases businesses reputation
- To what extent does conflict affect the development of secret communication using computers?
- What are the benefits and risks of AI in the modern day?
- To what extent can artificial intelligence replace humans in penetration testing?
- To what extent can an organisation be fully secure when it contains human users?
- Are black box and white box penetration tests an effective way of considering a system's security?
- How will the development of Quantum Computing affect data security on a national level?
- How Operational Security evolved over time
- Do cyber criminals target a particular profile of victims?
- What are the ethical considerations surrounding the use of artificial intelligence in cybersecurity?
- The history and evolution of cybercrime and the impact it has had on the development of interconnected technologies and networks
- What are the cyber security issues individuals and organisations faced within cloud and network data storage?
- Testing and monitoring measures used in cyber security. History, background and future testing and monitoring measures and the impact of these measures
- Is ethical hacking truly ethical or even secure? Investigation into Pen Testing as an ethical hacking mechanism and comparison with other ethical hacking methods * Cyber security aspects of VPNs and evaluating their effectiveness

---

2023-24

- What is the impact of artificial intelligence on Cybersecurity and what are the emerging trends?
- How does phishing affect companies, individuals and what can be done to prevent it?

- What awareness do young people have of cybersecurity threats and the preventative actions they should take? How can my school improve the education for its students?
- An analysis of Password Security and Multi-Factor Authentication in Cyber Security
- How vital is our Digital Footprint in an Ever-changing Digital Age?
- Mind Games in Cybersecurity: How do the human aspects of cybersecurity shape and impact the field including the use of psychology and media coverage?
- The War of the Future: How Digital Disinformation Threatens Democracy
- Exploring Educational Keylogger: Unveiling Development, Detecting Intrusions, and Fortifying Defence
- How are we able to ensure Security awareness for our public in this digital age, against the threat of cybercrime?
- The role of Ethical Hacking in compliance with industry standards and regulations.
- Augmented Security considerations to vulnerabilities in the gaming of the past, present and future
- Why Is the Use of Artificial Intelligence Important in Today's World of Cybersecurity?
- How can the uncontrolled growth of Artificial Intelligence influence the cyber security of an established organisation
- Identify and explain the potential risks that advanced Artificial Intelligence poses and will pose to cyber security, and consequently to humanity, and propose a potential solution
- What do we know about previous major cyber warfare attacks and what can we learn from them to better mitigate against cyber terrorism in the future?
- Central Bank Digital Currencies (CBDC) and Cryptocurrencies: Analysing the Threat to British Financial Information Security
- What action should the defensive cyber security industry take in order to mitigate the risk posed by a threat actor with access to a quantum computer?
- Businesses face a lot of security threats, which methods are most effective in trying to prevent these threats?
- Is security testing helping to reduce the number of successful cyber attacks?
- How effective is digital forensics in prosecuting cybercrime?
- Security testing and vulnerability assessment, how can these affect cyber in the present and future?
- How is Penetration Testing used in the Financial Sector to Protect Businesses?
- To research the impact of the Russian Business Network's cybercrime and compare them and their effects to that of modern-day attacks.
- How Significant is Ethical Hacking to Cyber Security in the Modern Day?
- Why are ransomware attacks increasing? And how can we minimise the impacts?

- Is Biometric Authentication the Future of Security?
- The rivaling history of Cyber Security and Malware Data concept
- In what way has the internet of things affected the security of devices and networks in homes?
- To what extent are the cybersecurity challenges within the gaming industry unique?
- Will the development of quantum computers mean that modern cryptographic techniques need to be revised?
- How does the Internet of Things pose a security risk?
- Beyond the Game: Examining the Concerns in Steam's Backdoor Casino and Gambling Sphere
- How can Artificial Intelligence assist humans in the detection of vulnerabilities and threats to computer systems for protection against cybercrime?
- How can AI be manipulated to commit cyber-crimes?
- Can we ever protect our identity online?
- In our ever-evolving society, will progress be halted in the wake of quantum computing and the danger it poses on worldwide cryptography and confidential communication?
- Should companies create “backdoors” in their devices for government agencies
- Are passwords enough, and will advancements in computing power surpass the level of protection your passwords can offer?
- Alan Turing – How embedded is his knowledge in Cryptography?
- Evolution of investigative tools and Anti-investigative tools and how they affect computer forensics. How can we be certain that a device hasn’t been hacked?
- Does politics influence cyber-crime and security?
- What are black hat hackers? Why do they do what they do and how do they do it?
- The Human Factor: Social Engineering
- Deepfake Technology – How can we protect ourselves in a world where seeing is no longer believing?
- Do Quantum Computers threaten Cryptographic Algorithms and Encryption? And considering the legal and ethical threats to society and the future quantum Computing entails.
- To what extent can deepfakes be used in criminal activity?
- Is there a possibility for AI to become a new competitor, or another obstacle in the way of mass surveillance, and what steps are being taken by governments to prevent anonymity?
- Encryption: How secure are our messages and our data, what threats do quantum computers impose on modern cryptography, and can the threats be countered?

- How will quantum computers change the future of cryptography, and how will it threaten traditional encryption?
- Should AI have the same legal rights as humans?
- Evaluate the impacts of different online privacy tools such as TOR on cybersecurity.
- How effective are cryptography algorithms for encryption and obfuscation of data against human and artificial intelligence decryption?
- How Will Quantum Computers Impact Encryption Algorithms?
- Which factor has been the most significant in enabling social engineering attacks?
- What is the best encryption method to protect against quantum computing?
- Virtual Penetration Testing: Successes, Flaws, and Alternatives
- Are biometrics a technologically strong enough barrier for protecting our data?
- How may quantum computers affect information security?
- Quantum computing will break modern encryption- or will it?
- To what extent will advancements in ML impact on network security?
- What are the implications of Remote Code Execution vulnerabilities for network security, and what steps can be taken to prevent them?
- How emerging technologies could change how companies protect data from external attacks.
- How important is penetration testing? an evaluation on penetration testing, and the significance it has in the cybersecurity sector.
- How does social bias affect the functionality of cyber security systems?
- To what extent are the impacts of cyber attacks damaging and expensive? How much sophistication is needed for a cyber attack?
- What might be the implications for the future of cryptography and data security given the current and potential future advancements in quantum computing?
- Can hacking ever be ethical?
- How does cybercrime and cybersecurity affect the music industry
- AI Anthropomorphism: Unveiling the Dark Side of Blurring the Lines Between Humans and Machines
- To what extent has progress in cybersecurity helped to reduce the vulnerability of financial institutions to a cyber-attack?
- Can cybersecurity keep up with cybercrime in the modern era of computing?
- What impact does AI have on the online world and cyber security in themodern day?
- Can social media services be trusted with user data?
- Hacktivism: Social Justice Tool or Weapon for Terrorists
- How may Artificial intelligence be used in and effect the Cyber security industry?
- Will the implementation of AI within cyber threats and cyber security tools make

the world overall more or less cyber secure?

- Delving into the World of Cybercrime and Cybersecurity: Understanding the Threats and Strategies for Prevention
- How will Artificial intelligence & neural networks affect the future of encryption?
- How is physical security tied to cybersecurity, and how can this challenge be managed?
- How will Quantum Computing affect the security of Blockchain technologies?
- Are nature inspired solutions an effective approach to mitigating current and future cyber security risks?
- Evolution of Malware. A review on past, present and future information security breaches.
- The Evolution of Digital Forensics and How It can Help Fight against Cyber Crime
- Cybercriminals: An investigation on different type of cyber attackers, their motives, background and characteristics
- An Examination of the Evolution of Cryptography and Cryptoanalysis in the 1960s
- Mis- and Disinformation in Cybersecurity Advertising
- How to prevent zero-day phishing?
- Helping people understand Asymmetric encryption
- Implementations of machine learning for DDoS attack prevention and anomaly detection in cybersecurity
- How is the public put at risk by cyber attacks on Critical National Infrastructure?
- Understanding and Mitigating the Risks of Penetration Testing Tools in the Wrong Hands
- How does digital forensics follow suspect’s digital evidence?
- Can our personal information be compromised through communication with a chatbot and where does the training data for the AI come from?
- How are digital forensics used, analyzing the stages of the process through the use of case studies.
- Investigation into the deep/dark web and if the anonymity it provides is the most secure way to use the internet
- Evaluating the effectiveness of VPNs
- Brute Force Attacks on Passwords: How effective are they in the modern day
- A detailed investigation into the risks and potential security flaws of device hardware-based encryption on multiple popular consumer platforms.
- Evaluating the effect of AI on Britain’s economy and cyber security
- Will rapid development in AI more beneficial to cyber analysts protecting our systems or hackers with malicious intent and therefore be banned altogether?
- How can embracing Emerging technologies and Ethical hacking help strengthen Cyber security against cyber threats?
- Should the UK establish a national e-governance mobile application and, if so, what security measures and benefits will there be?

- How IoT devices use protocols to work together and the implications of mass development of IoT devices on the landscape of cybersecurity
- Are cyber operations an effective weapon in interstate conflict?
- How secure is biometric authentication compared to other forms of authentication, such as password based or token based authentication?
- How can small businesses protect themselves from Cyber-Attacks?
- Can you ever be truly anonymous online?
- How secure is our messaging and how has that security evolved?
- How has encryption evolved and can it survive in the age of quantum computing?
- Will passwords outlast digital forensics?
- Are the current tools an effective threat against cybercriminals?
- Can the illegal actions that Anonymous take be considered a justified form of civil disobedience?
- Do recent technological advancements in cashless transactions help or hinder crime prevention?
- In what ways could artificial intelligence be a detriment or benefit to cybersecurity?
- Should cyber criminals be punished according to intent or action?
- How detrimental can Online Impersonations be?
- How cyber security and digital forensics are interlinked industries that are dependent on each other for conclusive outcomes on solving cybercrimes?
- Cyberterrorism and the global threat it poses: Exploring some of the consequences
- How has digital forensics developed over time: past, present, and future?
- Exploring the Role of VPNs in Online Security and Privacy.
- How has the improvement in AI affected social engineering?
- A report on the dangers of packet sniffing and vulnerabilities that it can lead to.
- Regulation of the cyberspace and its effects over statecraft: how are international relations effected by this?
- Quantum computers: How do they work and are they the future of vulnerability testing?
- How malicious actors employ fake accounts as a tool to commit various cyber crimes, and how this has changed over time
- An insight into the world of penetration testing
- The implications social engineering has on organisations and individuals
- How do cyber-attacks leak the unethical activities in international organisations? Are these hackers working for the people or personal gain?
- To what extent does machine learning impact on an IOT security strategy for business
- To what extent will AI help protect data and keep it secure?

- How and to what extent is ethical hacking ethical?
- How will the evolution of digital security directly impact the development and threat posed by viruses in the future?
- To what extend do governments monitor their citizens using technology to prevent cybercrime, and do the associated negatives outweigh the positives?
- To what extent will current technological issues fuel the changes to potential trends in cybercrime?
- To what extent will AI influence the way in which we can protect ourselves against cyber-crime?
- Does the threat of quantum computing make blockchain unsafe and untenable to use in the future?
- To what extent do social engineering attack affect modern society?
- To what extent can cyber attacks be improved by utilising the features of AI
- The history of cybercrime, what tools they used and how they were used
- Secure Software Development
- Can artificial intelligence replace humans in penetration testing in the Internet of Things
- What are the values and consequences of 'backdoors' in end-to-end encryption?
- The history of cyber encryption and how it has evolved over time
- The history of cybercrime and how it has evolved over time
- Safety of gaming communities and how secure they are against cyber crime
- What are VPNs and how should they be used
- The impact of cyberwarfare on MI5: challenges and response
- Could artificial intelligence replaces human penetration testing
- Are online gaming communities protected from modern cybercrime?
- Kali Linux tools and their complex uses
- Human error within the disposing of confidential data
- A psychological profile of a hacker
- What is the purpose of creating cyber security incident reports and the consequences of ignoring and not acting on them?
- Cyberwarfare – UN proposed conventions on cybercrime, and damages cybercrime can cause to the average person without proper regulation
- The Impact of Cryptocurrency on Cybersecurity
- What was the impact of the WannaCry attack on the UK?
- How effective is penetration testing and whether the disadvantages outweigh the benefits of it?
- How big of a threat is anonymity through the TOR browser to Organisations/individuals?
- How safe are our cities against targeted attacks on individuals?
- How feasible it is to mark identity online using VPNs?

> - What are the types of people that commit/prevent cyber attacks and what are they types of cyber-attacks? What can we do to prevent them from happening now?
> - How cybersecurity is evolving with aspects of cyber viruses and cyber-attacks?
> - What Factors Other Than Monetary Gain Drive Young Cyber Criminals into Cybercrime?
> - What are Propaganda Attacks within cyberwarfare and how can they affect national security of the UK?

Can you put together a title that will allow you to investigate and access the higher-level concepts and skills : plan, research, analyse, evaluate & explain

Project Titles 2020-21.pdf (cyberepq.org.uk)

A* example for you to look at Course: Cyber EPQ 1 Year Course 2025-26, Topic: Project Writing Assistance

---

What does the project need to allow me to include?

- **Identify, design, plan and complete an individual project**, applying a range of organisational skills and strategies to meet agreed objectives.
- **Obtain, critically select and use information from a range of sources**; analyse data, apply it appropriately and demonstrate understanding of any relevant, connections and complexities of the topic.
- **Select and use a range of skills**, including new technologies, solve problems, take decisions critically, creatively and flexibly, to achieve planned outcomes.
- **Evaluate outcomes** both in relation to agreed objectives, as well as own learning and performance.
- **Select and use a range of communication skills and media** to present evidenced outcomes and conclusions in an appropriate format.

Research / Evaluation Table of Resources

In order to achieve high marks you need to build on the work of others without

An Evaluation Table of Resources is an acceptable way to evidence how resources have been evaluated throughout the project. This can be done as a spreadsheet and may look like

this. When completing how useful the source was, it could be beneficial to evaluate the strengths and weaknesses of the source, as well as how it was used in your project

Source Type	Source	Author	Date Published	Publisher (Books Only)	Date Accessed	Was it useful?

Checking your idea

- Is the title clear and focused on an issue which can be managed:
  - within the timescale, available resources and word total?
- Do the title and proposed action plan indicate that you will be capable of:
  - investigating and researching the topic or carrying out the activity or task independently?
- Is there a danger that you will be unable to approach the project impartially and in a balanced way?