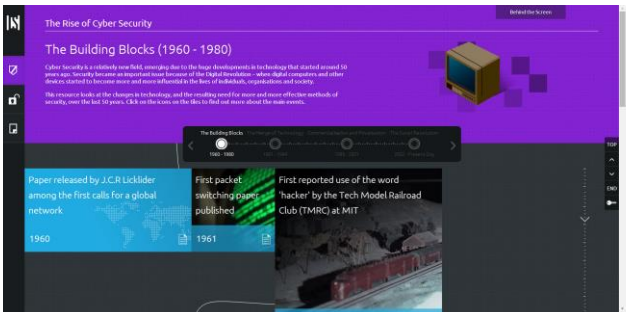
Getting Started with CSA

Making the most of this project

The purpose of CSA

The purpose of Cyber Security Advanced (CSA) is to extend your understanding of cyber security and give you a real insight into the work that cyber security professionals are involved in. You may be studying this as part of an A level or other qualification, or just exploring it because you are interested in a possible career in Cyber Security (a career option with huge opportunities, a potentially very good salary, and increasing number of vacancies!) or because you want to know that you are safe and secure in your own online world.



The Rise of Cyber Security

The Building Blocks (1960 - 1980)

Cyber Security is a relatively new field, emerging due to the huge developments in technology that started around 50 years ago. Security became an important issue because of the Digital Revolution – when digital computers and other devices started to become more and more influential in the lives of individuals, organisations and society.

This resource looks at the changes in technology, and the resulting need for more and more effective methods of security, over the last 50 years. Click on the icons on the tiles to find out more about the main events.

Paper released by J.C.R Licklider among the first calls for a global network
1960

First packet switching paper published
1961

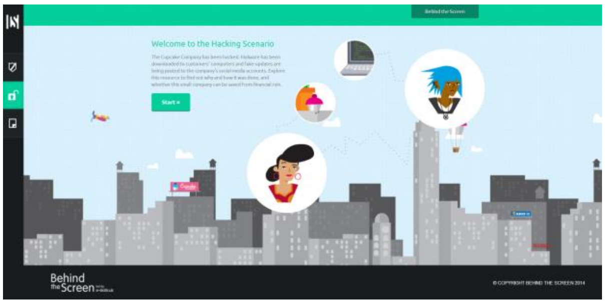
First reported use of the word 'hacker' by the Tech Model Railroad Club (TMRC) at MIT

You may have already studied the Countdown to Chaos module, or the Key Stage 4 materials on TechFuture Classroom, so have some insight already into the importance of cyber security and its relevance to everyone who uses technology. CSA explores many of the topics in much more detail, and will provide you with more insight into real life security issues, cyber crime and the methods used to fight it, and how businesses deal with the risks of cyber attacks and their potential after-effects.

The structure of the CSA project

The CSA project consists of five e-learning modules, four relating to a timeline of technological and cyber security development, together with a real life hacking scenario. Each of these opens in a new window in your browser – so close the window to return to the course page. These five modules map to ten cyber security content modules in this project, and the table below shows how the content of the whole project maps on to the learning outcomes across the ten areas of cyber security.

The learning outcomes are delivered through two sections – the Timeline and the Hacking Scenario. The Timeline maps the history of technological development in four eras and how cyber security has had to run in parallel to deal with the security consequences of changes in the way we run our lives and use technology more. The Hacking Scenario details the effects of a cyber attack from the perspective of a small business owner. This also includes some insight into the minds of both the owner and the unethical hacker, including psychological profiles. In the end, cyber security is about understanding people as much as about understanding technology, so we have made sure we cover this as well in this project.


Behind the Screen
Welcome to the Hacking Scenario
Start »
Behind the Screen
© COPYRIGHT BEHIND THE SCREEN 2014

The Cupcake Company has been hacked. Malware has been downloaded to customers' computers and fake updates are being posted to the company's social media accounts. Explore this resource to find out why and how it was done, and whether this small company can be saved from financial ruin.

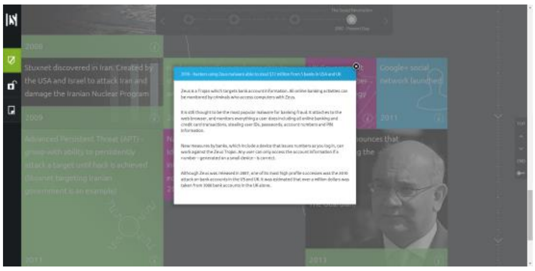
You can work methodically through this, perhaps with guidance from your teacher, and use the assessment materials provided in the Resources area to test your knowledge. Or you can try the Timeline Quiz to find out more about the history of cyber security and how it as developed in parallel with key technological changes. Make sure, though, that you check out the Hacking Scenario as well as the Timeline – awareness of the real life consequences of a cyber attack is important knowledge for a cyber security professional – something you may well become one day!

Using the Timeline

The Timeline is sub-divided into four eras. These are:

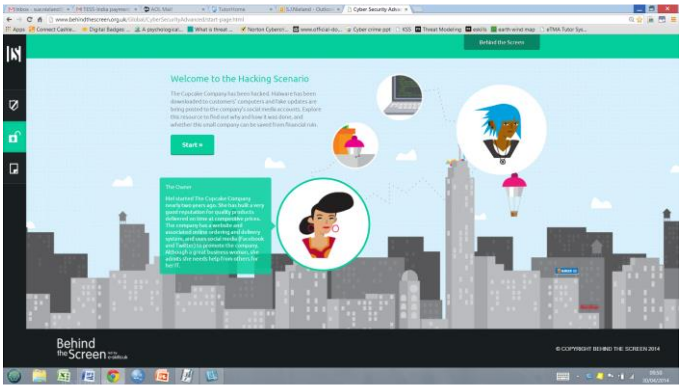
1. The Building Blocks, between 1960 and 1980

2. The Merge of Technology, between 1981 and 1994
3. Commercialisation and Privatisation, between 1995 and 2001
4. The Social Revolution, between 2002 and present day


Stuxnet discovered in Iran. Created by the USA and Israel to attack Iran and damage the Iranian Nuclear Program
Advanced Persistent Threat (APT)
Google social network launched
2011

Within each era, there are tiles that represent key milestones. Each has pop up information, a document or video with more detail about each event. Using the Timeline Quiz is a great way to find out more about the Rise of Cyber Security. You will find it in the Resources area of the site under Assessment.

Using the Hacking Scenario



Welcome to the Hacking Scenario

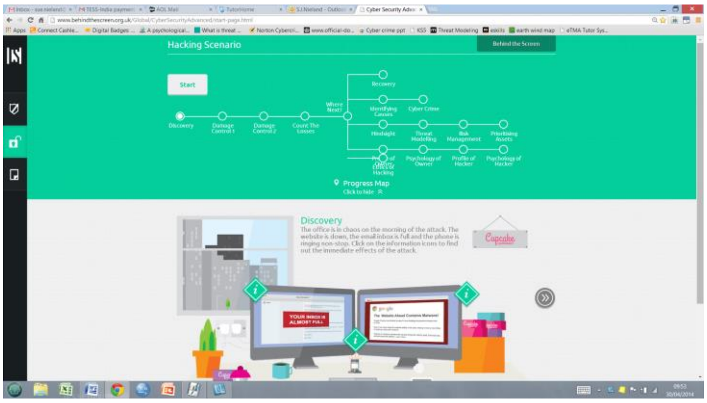
The Cupcake Company has been hacked. Malware has been downloaded to customers' computers and fake updates are being posted to the company's social media accounts. Explore this resource to find out why and how it was done, and whether this small company can be saved from financial ruin.

The Owner

Mel started The Cupcake Company nearly two years ago. She has built a very good reputation for quality products delivered on time at competitive prices. The company has a website and associated online ordering and delivery system, and uses social media (Facebook and Twitter) to promote the company. Although a great business woman, she admits she needs help from others for her IT.

The hacking scenario tells the story of a cyber attack on a small business. It starts with the two main characters – the owner and the hacker. Roll the mouse over the images of the two to find out more about the background to the attack.

Clicking on Start will take you into the Discovery section. Information icons give pop up information about the attack either as text or audio.



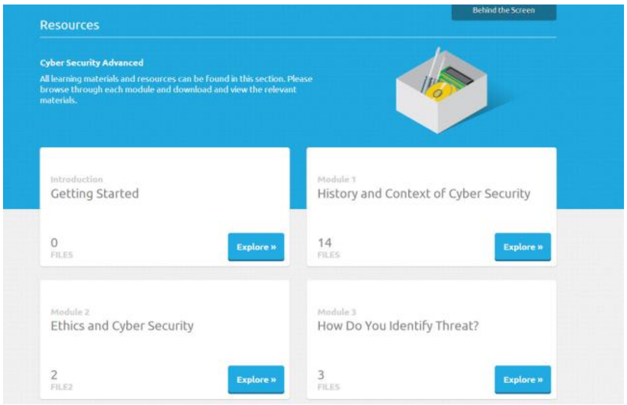
Discovery

A progress map, showing the route through the Hacking Scenario, will drop down from the top when clicked. You can work through the scenario using the map, or click through using the arrows. When you have reached the Count the Losses page, you then have a choice to explore other issues around the attack including what could have been done to avoid the attack (Hindsight), how the company recovers from the attack, and more about the people involved. Under the Identifying Causes section you can find out more about cyber crime and how the police and other agencies deal with the increasing number of cyber criminals who are launching cyber attacks from across the world. Links from the text will open up documents with much more information.

Assessment tasks are also provided. You can model threats that a company faces, plan a security strategy for a small business, consider risk assessments and understand more about information assets and their prioritisation. At the end of this project, you will have an advanced understanding of cyber security and will be in a great position to seriously consider a career in this field. You could even end up being employed by the government's security agency, GCHQ – we have included information in the project about the careers available at this agency.

The Resources page

All of the documents, including the Timeline Quiz and other assessment tasks, are available in the Resources module (scroll along the e-learning modules to find them). These are categorised under modules so you can see how the documents relate to the learning outcomes for each. More information about this is in the table on page 5 (below).



Resources

Cyber Security Advanced

All learning materials and resources can be found in this section. Please browse through each module and download and view the relevant materials.

Introduction
Getting Started
0
FILES

Module 1
History and Context of Cyber Security
14
FILES

Module 2
Ethics and Cyber Security
2
FILE2

Module 3
How Do You Identify Threat?
3
FILES

Enjoy working on TechFuture Classroom Cyber Security Advanced! If you have any comments to share with us about working with this project and whether it inspires you to find out more about cyber security careers, we'd love to hear from you at learning@thetechpartnership.com.

Modules and Learning Outcomes mapped to content

Module	Learning outcomes	Location in project	Related resources	Assessment
Module 1: History and context of cyber security	Understand why cyber security is important including a history of the development of cyber threats	Timeline (all eras)	Module 1 resources	Timeline Quiz
	Understand geopolitical drivers, cyber espionage and the rise of cyber warfare	Timeline (1995 to present day)	Module 1 resources	Timeline Quiz Essay Questions
	Know the importance of intelligence and its role in counteracting cyber attack	Timeline (1995 to present day)	Module 1 resources	Timeline Quiz
	Understand the real impact of losses due to cyber attack	Timeline, Hacking Scenario (counting the losses)	Hindsight documents – Disaster Recovery Psychology of the owner	Timeline Quiz
	Recognise the unintended consequences of the rise of technological trends	Timeline	Module 1 resources	Essay Questions

Module	Learning outcomes	Location in project	Related resources	Assessment
	Know the legislation in the cyber security industry including international standards and their implications for individuals and organisations	Timeline (1981 – present day)	ISO 27001 Computer Misuse Act	Timeline Quiz Essay Questions
Module 2: Ethics and Cyber Security	Understand the importance of ethical behaviours for security professionals	Hacking Scenario (people involved section)	The Ethics of Hacking	Essay Questions
	Know what is ethical behaviour and what is not	Hacking Scenario (people involved section)	The Ethics of Hacking	Essay Questions
	Understand the difference between ethical and unethical hacking	Hacking Scenario (people involved section)	The Ethics of Hacking	Essay Questions
Module 3: How to you identify threat?	Be familiar with different forms of threat modelling	Hacking Scenario (hindsight section)	Threat Modelling	Task: Model the threat in a small business
	Be able to model threat against an application or system	Hacking Scenario (hindsight section)	Threat Modelling	Task: Model the threat in a small business

Module	Learning outcomes	Location in project	Related resources	Assessment
Module 4: Vulnerabilities – understanding how the bad guys break in	Understand the different types of typical attack including phishing, social engineering, website compromise, malware, network interception and weak authentication	Timeline Hacking Scenario (identifying causes section)	Module 4 Resources	Essay Questions
	Understand how experts address issues of vulnerability in a real life context	Hacking Scenario (identifying causes section)	Module 4 Resources Security Technologies Risk Assessment	Essay Questions Risk Assessment Task
Module 5: Principles of risk management	Understand the basic concepts of risk management	Hacking Scenario (hindsight section)	Risk Assessment	Risk Assessment Task
	Carry out a risk assessment on a system	Hacking Scenario (hindsight section)	Risk Assessment	Risk Assessment Task
Module 6: Understanding a	Know the range of assets that have to be protected within a typical business	Hacking Scenario (hindsight section)	Understanding and prioritising information assets	Prioritising assets task

Module	Learning outcomes	Location in project	Related resources	Assessment
business and prioritising resources	Understand how to use a prioritising technique by identifying the importance of information assets	Hacking Scenario (hindsight section)	Understanding and prioritising information assets	Prioritising assets task
	Apply a prioritising technique to a small business	Hacking Scenario (hindsight section)	Understanding and prioritising information assets	Prioritising assets task
Module 7: Human factors in cyber security	Understand the role of human behaviour in cyber security	Timeline Hacking Scenario (people involved section)	Profile of the owner Profile of the hacker	Essay Questions
	Understand and apply the need for education in security awareness	Hacking Scenario (hindsight section – cyber security training)	Staff training in cyber security	Essay Questions
	Identify and practice secure behaviours	Hacking Scenario (hindsight section)	Module 7 resources	Essay Questions
Module 8: Security technologies	Identify a range of common security technologies	Timeline Hacking Scenario	Module 8 resources	Essay Questions
	Understand the use of firewalls, hard drive encryption, dual factor authentication, VPNs, Information	Hacking Scenario	Security Technologies	Essay Questions

Module	Learning outcomes	Location in project	Related resources	Assessment
	Rights Management, Identity and Access Management and the role of the Cloud Security Alliance in security			
Module 9: Business Continuity Management	Understand how organisations continue business after a cyber attack	Hacking Scenario (Recovery)	Module 9 resources Profile of the owner	Essay Questions
	Identify methods by which organisations can recover including use of back up, remote servers and cloud technology	Hacking Scenario (Recovery)	Module 9 resources	Essay Questions
Module 10: Designing an Information Security Management System	Understand the ISO 27001 standards and why they are needed	Timeline (2005)	ISO 27001	Design a security strategy for a small business
	Design a security strategy for a small company	Hacking Scenario (all)	Security Technologies Website Maintenance (Module 9) Module 4 resources	Design a security strategy for a small business