Royal Academy of Engineering

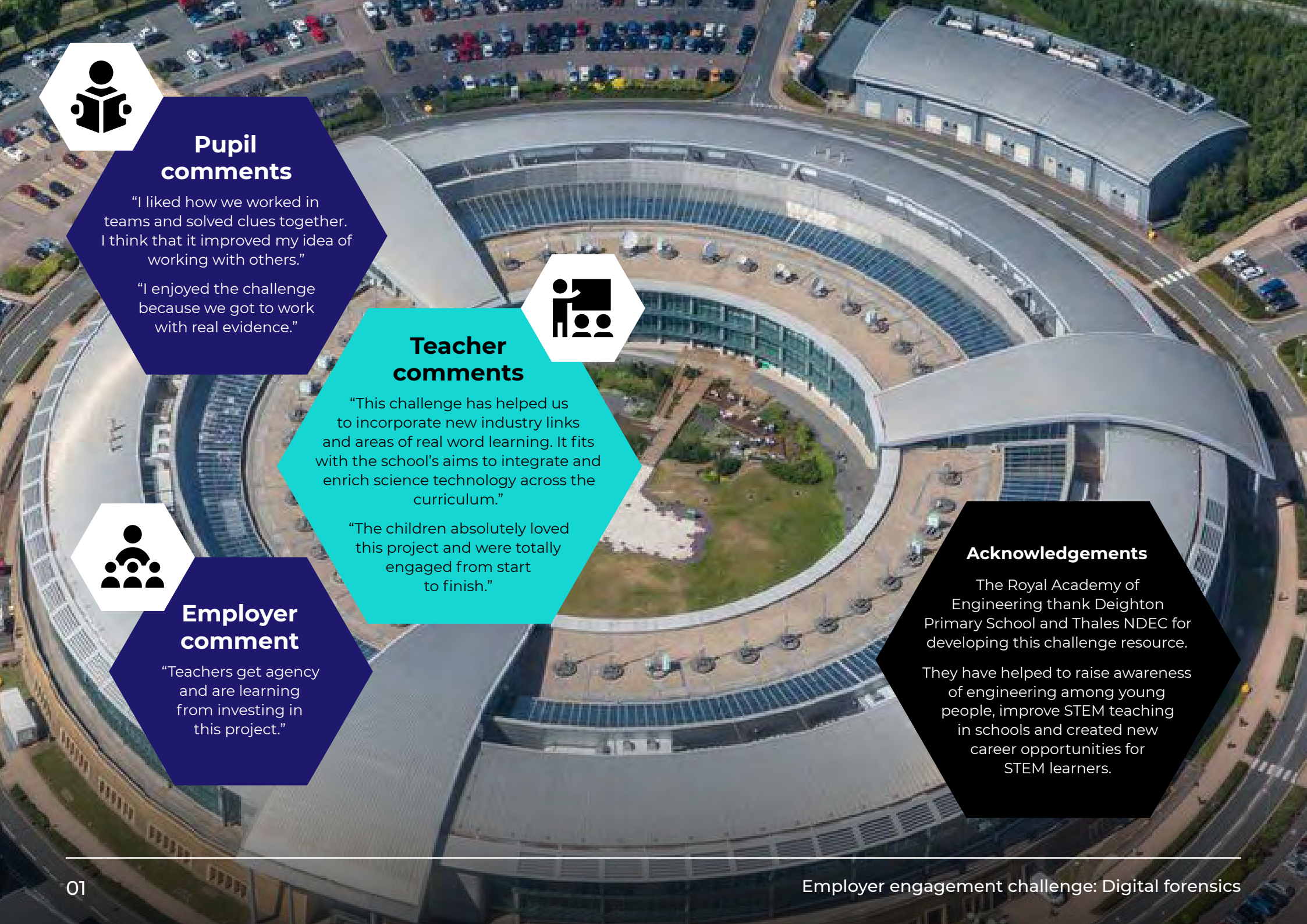
Employer Engagement Challenge

Digital forensics

Are you a 21st Century Sherlock Holmes?

Ariennir gan **Lywodraeth Cymru**
Funded by **Welsh Government**

THIS IS ENGINEERING



Pupil comments

"I liked how we worked in teams and solved clues together. I think that it improved my idea of working with others."

"I enjoyed the challenge because we got to work with real evidence."

Teacher comments

"This challenge has helped us to incorporate new industry links and areas of real word learning. It fits with the school's aims to integrate and enrich science technology across the curriculum."

"The children absolutely loved this project and were totally engaged from start to finish."

Employer comment

"Teachers get agency and are learning from investing in this project."

Acknowledgements

The Royal Academy of Engineering thank Deighton Primary School and Thales NDEC for developing this challenge resource.

They have helped to raise awareness of engineering among young people, improve STEM teaching in schools and created new career opportunities for STEM learners.

Thales NDEC

Thales and the National Digital Exploitation Centre (NDEC) is a cyber centre of excellence with a mission to protect Wales from cyber threats and develop the cyber experts of the future.

NDEC is the first research and development facility in Wales and provides local, regional and national organisations with the digital security infrastructure required in an increasingly complex technological world.

The challenge

During this investigative challenge, young learners will experience what it is like to become 21st century detectives. Working in teams, they will develop their digital forensics skills, collect and analyse evidence to solve a mysterious wrongdoing, and learn about cybercrime, cyber law and the importance of online safety and behaviour along the way.

They will use the context of a crime scene to make connections across the science and technology curriculum and beyond, developing their analytical skills by observing the rules of a crime scene, collecting evidence, decoding ciphers and scrutinising data.

Each team member is assigned a specific role – searcher, note-taker, photographer, evidence bagger and evidence logger. They will learn about the different types of evidence and how to collect it, as well as the tools and techniques used to analyse evidence and investigate a real-world case using digital forensic techniques. The challenge culminates in a mock court case and is a great way for pupils to see how these skills can be used in the real world.

This challenge is designed to support practitioners to follow Curriculum for Wales' careers and work-related experience guidance. It is supported by a set of videos that give an inside look at how engineers at Thales NDEC work, and introduces first-hand how the challenge is delivered in school.

The challenge is recommended for primary school pupils and can be adjusted to match different age groups and abilities.

Teachers should use discretion when incorporating internet safety and cybercrime into their lessons. Carefully review the material and determine the appropriateness of the activities to ensure its suitability for the age group you are teaching.

Here are some of the learning opportunities that the challenge provides:

- **Collaborative teamwork**
- **Scientific investigation**
- **Public speaking**
- **Problem finding and solving**
- **Digital safety and security considerations**

Challenge overview

Setting the class challenge

Get ready for an investigative journey into the world of digital forensics. Thales NDEC would like your help to solve a mysterious cybercrime.

One of Thales NDEC's hi-tech electric cars has been the victim of a hacking attack and a memory stick containing all the car's essential data has been stolen. The memory stick holds the key to the car's operations and functionality and without it the vehicle is immobilised and inoperable.

Step into the shoes of cyber investigators and problem-solvers, helping Thales NDEC identify and bring the hacker behind this cyber intrusion to justice.

Your expertise in various scientific and technological disciplines, plus your understanding of cybercrime, cybersecurity, and encryption makes you the perfect group to assist in this investigation and unravel the mystery.

The Progressing to be an Engineer cycle

By participating in this challenge, young learners will develop the skills and practices that engineers use every day in their professional lives.

Asking questions, imagining and planning ideas, creating and refining outcomes, while continuously reflecting on how things could be improved, are all 'Engineering Habits of Mind' as demonstrated in 'the Progressing to be an Engineer' cycle.

Learning opportunities	Core skills
■ Collaborative teamwork ■ Scientific investigation ■ Public speaking ■ Problem finding and solving ■ Digital safety and security considerations	**Literacy:** Reading and technical vocabulary. Selective research. Writing and reporting. Presenting and communication. **Numeracy:** Data collection and analysis. Pattern spotting. Measurements and calculation. **Scientific:** Problem-solving and experimenting. Visual and special awareness. **Technical:** Systems thinking and problem-solving. Communication and teamwork.

	Activity	Success will look like
0–2 hours	**Watch the challenge videos** – engineers films **Research** **Time to play** – Interland Internet safety **Time to research** – potential risks and challenges presented in the digital world **Time to present** – findings from the cyber research	Understand the aims and requirements of the challenge, as well as how digital forensics and cyber investigation relate to it Gather relevant information and have a clear and comprehensive understanding of the challenge. Present with confidence in the role. The presentation will be clear, well-structured and persuasive.
2–4 hours	**Cryptography** **Time to encrypt and decrypt** ***Decode*** – Ciphers table and wheel **Steganography** **Time to decrypt** ***Decode*** – hidden message	Recognise patterns, identifying encoded messages and cracking secret code. Use problem-solving and analytical skills to decode complex cryptography and steganography tasks. Assess the strength of encryption methods and identify potential vulnerabilities in cryptographic systems.
4–6 hours	**Crime scene investigation** **Time to observe** – the crime scene **Time to investigate** – the crime scene and evidence **Time to analyse** – the evidence	Comprehensive documentation, recording the necessary information without missing critical details. Effective communication and collaboration among team members. Accurate analysis, deriving valuable insights from the evidence.
6–8 hours	**The mock trial** **Time to prepare** – crime scene report **Time to present** – the evidence **Time for the verdict** – the court's ruling	Think critically and analyse the case. Evident in the quality of the report, presentation and questioning. Working well with the team, coordinating efforts and supporting each other's roles. Present with confidence in the role. The presentation will be clear, well-structured and persuasive.

Time to start

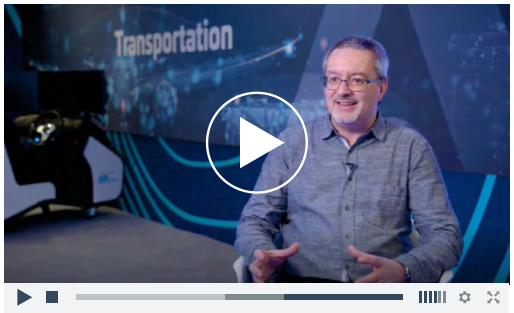
Begin by showing the class the set of three engineer videos that showcase the diverse range of engineering roles within the company. Each video is approximately three minutes long.

Go to **raeng.org.uk/wvep** or scan the QR code to watch the videos.

Connor: Cybersecurity apprentice

Dafydd: Cybersecurity apprentice

Dean: Operational technology engineer



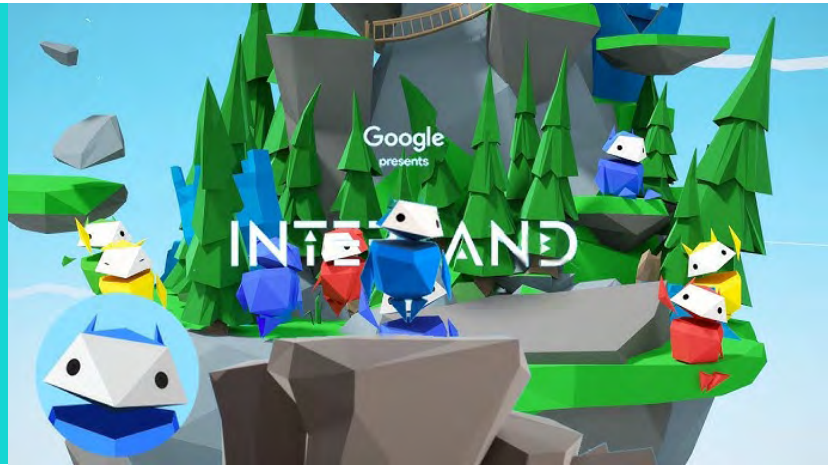
Time to play

Interland by Google: the aim of the first activity is to join an online adventure that teaches internet safety through four fun and challenging games.

Help fellow Internauts combat badly behaved hackers, phishers, oversharers and bullies by practising the skills needed to be good digital citizens.

In the game, players explore four floating islands: Kind Kingdom, Reality River, Mindful Mountain and Tower of Treasure.

Follow the link or scan the QR code to play the game and learn more about online safety.



https://beinternetawesome.withgoogle.com/en_us/interland

Time to research

The aim of this activity is to learn more about the potential risks and challenges presented in the digital world.

Start by discussing the increasing role of technology in our lives and the growing importance of the digital world.

Explain that as we embrace technology, we must also understand the potential risks and challenges it presents.

Time to research – *continued*

Divide the class into small groups of three or four pupils.

Each group will be responsible for researching one of the following topics: **cybercrime, cybersecurity or cyber law**.

Conduct online research to gather information about the assigned topic. Provide reliable sources such as government websites, academic institutions, or cybersecurity organisations.

For cybercrime research:

- What is cybercrime?
- Examples of common cybercrimes (e.g. hacking, phishing and identity theft).
- How does cybercrime impact individuals and organisations?
- How are cyber criminals typically prosecuted?

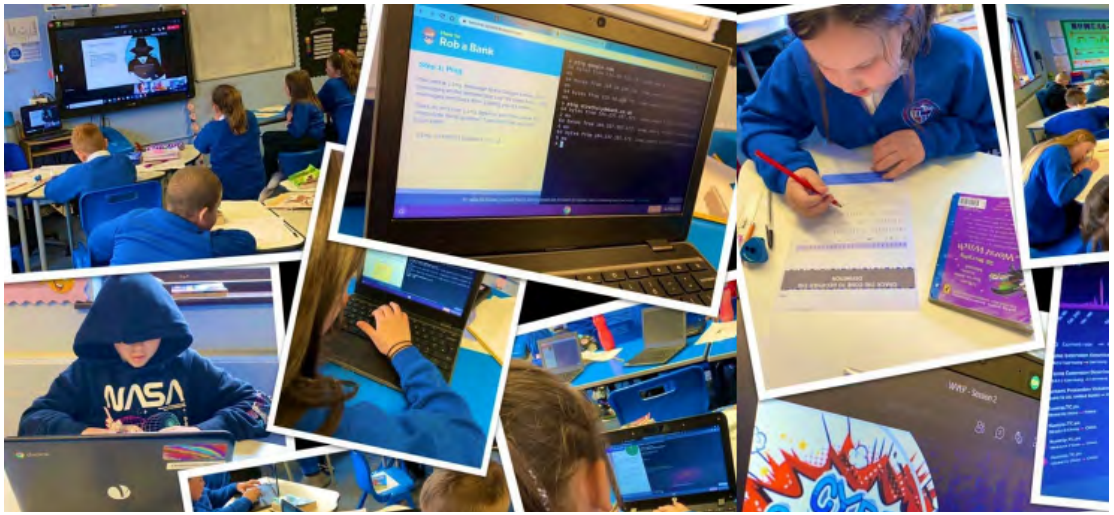
For cybersecurity research:

- What is cybersecurity?
- The importance of cybersecurity measures for individuals and organisations.
- Types of cyber threats and attacks (e.g. malware and traffic attacks).
- How can cyber breaches be prevented?

For cyber law research:

- What is cyber law?
- How are cyber laws developed and implemented?
- Key areas covered by cyber laws (e.g. data privacy and intellectual property).
- The role of cyber law with online behaviour and addressing cybercrimes.

Teacher: highlight that learning about cybercrime is to inform and empower pupils about online safety and potential cyber threats. It is not to create fear or alarm among them.



Time to present

Give each group an opportunity to present their findings to the class. They can use posters, drawings or verbal explanations to share the information they have found.

Encourage the other pupils in the class to ask questions and engage in discussions after each presentation.

Cryptography

The aim of this activity is to solve cybercrime using cryptography.

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it.

It has been used to code messages for thousands of years and continues to be used in bank cards and computer passwords in the digital world.

Below is a cipher encryption table.

Each letter of the UPPERCASE alphabet on the top row has been shifted forward four places so each letter matches to a different letter.

The alphabet has been shifted four places forward, therefore this is called a 'Cipher 4'.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d

We can then use this code to either encrypt or decrypt messages.

For example: the word **FORENSICS** becomes '**nwzmvaqka**' in code.

Time to encrypt and decrypt

1. First, encrypt the word **HACKER** using Cipher 4.
2. Next, start encrypting words and see if your team can decode them.
3. Then, it is time to start decrypting. Can you decode this message using a Cipher 2.

ygnn fqpg iqqf uvctv

Teacher: the decoded answers are on the last page

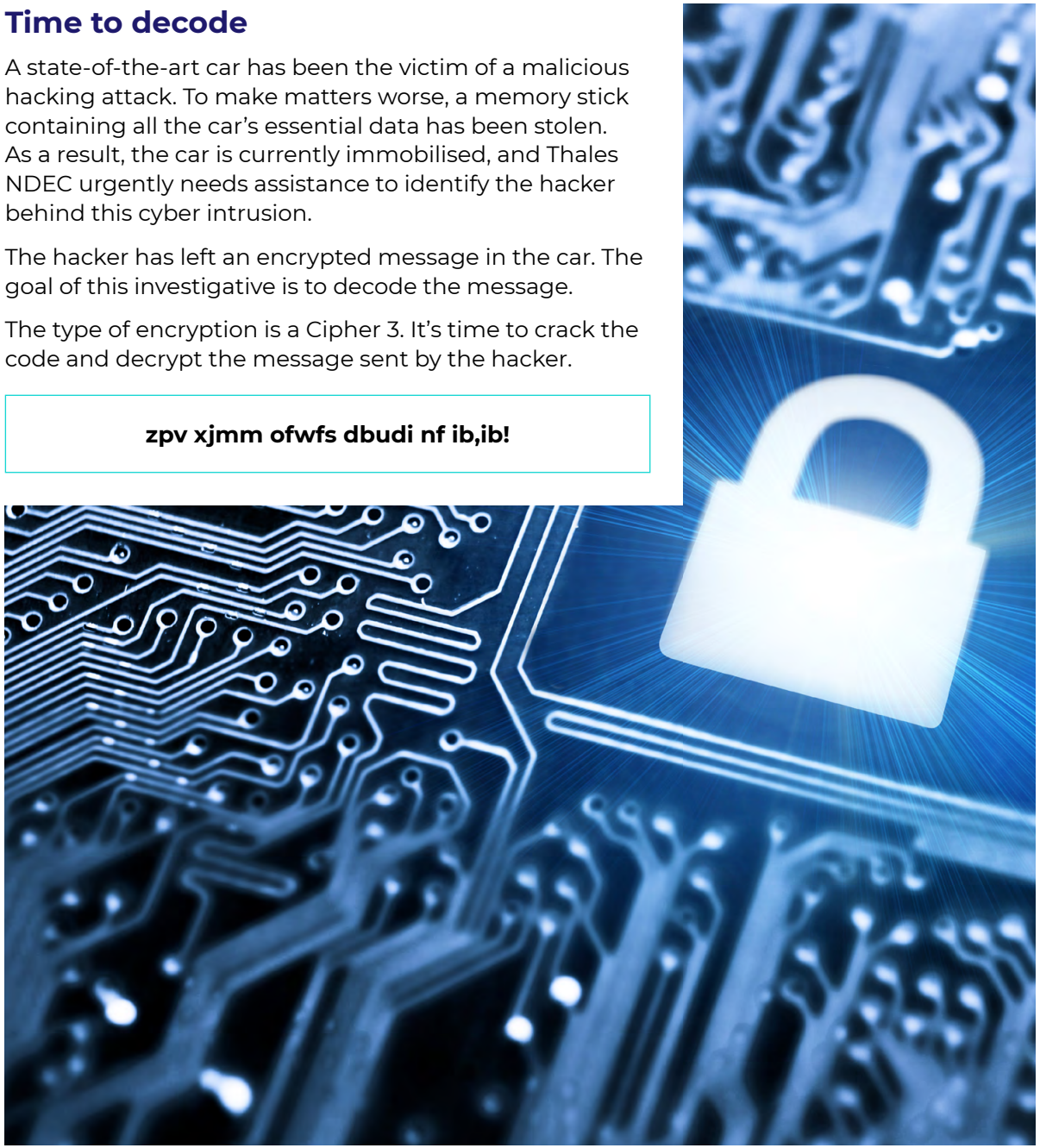
Time to decode

A state-of-the-art car has been the victim of a malicious hacking attack. To make matters worse, a memory stick containing all the car's essential data has been stolen. As a result, the car is currently immobilised, and Thales NDEC urgently needs assistance to identify the hacker behind this cyber intrusion.

The hacker has left an encrypted message in the car. The goal of this investigative is to decode the message.

The type of encryption is a Cipher 3. It's time to crack the code and decrypt the message sent by the hacker.

zpv xjmm ofwfs dbudi nf ib,ib!



Time to decode – *continued*

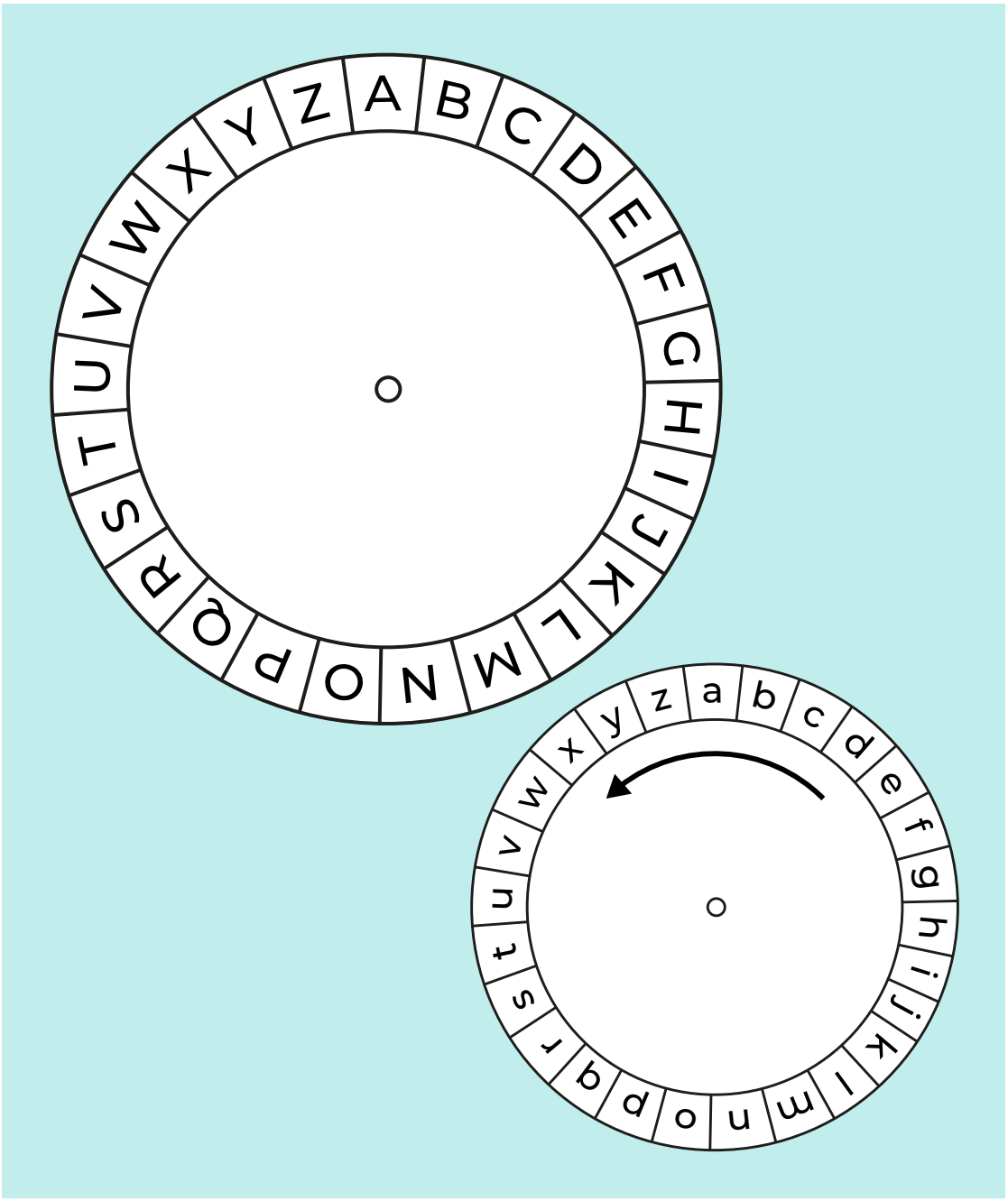
The hacker has sent another message. This time it will need to be decoded using a cipher wheel.

Making a cipher wheel

1. Photocopy and cut out the two (inner and outer) cipher wheels.
2. Fit the two wheels together one on top of the other, using a paper fastener pushed through the point that marks the centre of each wheel.
3. Turn the paper fastener round one complete turn to ensure the wheel can rotate smoothly.
4. Line up the wheels so that both ‘A’ and ‘a’ are matching.
5. Imagine that you have been given a Cipher 5 – turn the inner wheel five spaces to the left in the direction indicated by the arrow. Your wheel is now set up to decode.

Using a Cipher 5, can your team decode the next message?

jiz cpimzy kjpiyn ajm ocz hzhjmt nodxf



Time for some more decoding

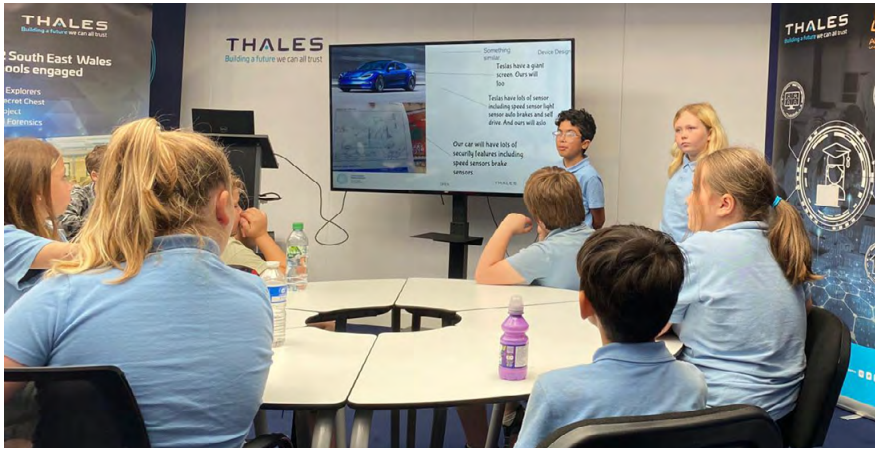
Steganography is a way of hiding information inside a picture or words.

Hackers use steganography to hide code, such as a virus that could corrupt a computer or immobilise a car from driving.

The hacker has left a final clue, but it is a steganograph in the form of encrypted symbols.

However, your teacher has intercepted a 'decoding key', which can be used to find the hidden message.

Decode the message and find out what the hacker wants.



Ενγινεερινγ λεαπε ιμπορταντ φορ α οφ, ανδ ιτσ σιγνιφιχανχε βαγ βε οβσερπεδ ιν πλαριουσ ασπεχτσ οφ μοδερν σοχιετψ. Ηερε μονεψ κεψ ρεασονσ.

Ιν συμμαρψ, ιν πιταλ, ανδ αδδρεσσινγ τηε χηαλλενγεσ οφ τηε σχηοολ ωορλδ. Ιτ ιννοπατιον, εχονομιχ μοδερν ρεχεπτιον, ιναβιλιτψ, ανδ ον ιμπροπεμεντ οηυμαν σατυρδαψ.

Decoding key

α	β	χ	δ	ε	φ	γ	η	ι	φ	κ	λ	μ
a	b	c	d	e	f	g	h	i	j	k	l	m

ν	ο	π	θ	ρ	σ	τ	υ	ϖ	ω	ξ	ψ	ζ
n	o	p	q	r	s	t	u	v	w	x	y	z

Time to observe the crime scene

The aim of this activity is to investigate the scene of the crime, finding clues to uncover the identify of the hacker.

> **Teacher:** Remember that you will eventually be suspected of the crime, charged and later sentenced in a school court of law.

Divide the class into teams of five pupils.

Each team will represent a digital forensic investigation unit with specific roles.

Teams will either select or be assigned a role from the table below. Ensure that they have all the necessary equipment, are familiar with their responsibilities and are prepared to undertake their respective roles.

Team role	Equipment	Responsibility	Key skills
Searcher	**Hazmat suit and number cards**	To look for and find at least three pieces of evidence	Attention to detail, thinks outside of box, good leadership and communication skills
Evidence bagger	**Hazmat suit and evidence bag**	To bag and store the evidence	Responsible, careful and organised
Note-taker	**Hazmat suit, notebook and pen**	To note down everything	Attention to detail, organised with good handwriting
Photographer	**Hazmat suit and camera**	To photograph the evidence	Good at taking pictures, careful and responsible
Evidence logger	**Hazmat suit, pen and pencil**	To fill in the log sheet and sketch evidence	Organised, good handwriting, responsible and a good drawer

Preparing the crime scene

Most schools do not have a state-of the-art autonomous vehicle, so use the school mini-bus as the “hacked” Thales NDEC car.

Before the forensic investigation begins, hide the following items inside the vehicle.

- A memory stick
- A handwritten note on filter paper – *written with a water soluble pen such as a Sharpie*

Additionally, you can add some incriminating evidence that leads to the teacher, or a red herring item to misdirect the teams, such as a random toy or unrelated object.

Cordon off the area around the vehicle using crime scene tape to create a sense of authenticity and to prevent any disturbance during the investigation.

Time to investigate

Each team member should wear a hazmat suit before approaching the crime scene to avoid contamination of evidence.

They should carefully search and examine the interior of the vehicle for any evidence related to the car hack.

When teams discover evidence, the **searcher** must mark the area with a number card, before the **bagger** carefully places it in a separate see-through plastic bag, making sure it is labelled with the appropriate item description.

As teams find evidence, the **note-taker** should record details about the evidence, its location within the car and any initial observations or theories. It is the job of the **evidence logger** to fill in a log sheet and sketch the items.

The **photographer** should take clear and detailed pictures of the crime scene and the evidence found inside the vehicle.

Sequence diagram of assigned roles and responsibilities

Materials

- Hazmat suits, number cards, notepad, log sheet, camera and plastic bags
- Crime scene tape, memory stick and handwritten note with the teacher’s marker pen

Analysing the evidence – chromatography

Chromatography is a technique used to separate the different pigments of ink that are present in a water-soluble marker pen.

Each type of ink tested will produce a unique pattern. This will determine that the ink used to write the note found in the vehicle is the same as the ink from the pen that belongs to the teacher.

Time to analyse

Provide each forensic team with five filter paper strips and four different coloured 'Sharpie' pens. **One of these strips (strip 1) should be a sample cut from the handwritten note found in the vehicle.**

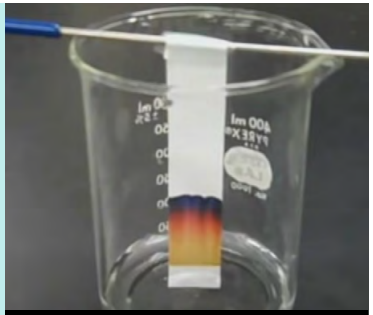
Draw a line approximately two centimetres from the end of each strip using a different coloured marker pen. **Strip 2 should be the same pen used to write the note on strip 1.**

Suspend the strip in a beaker with a small volume of water. The line should be slightly above the surface of the water.

What's happening?

The water starts to rise up the paper because of capillary action.

The ink will separate into different colours because the pigments in each unique pen has different properties.

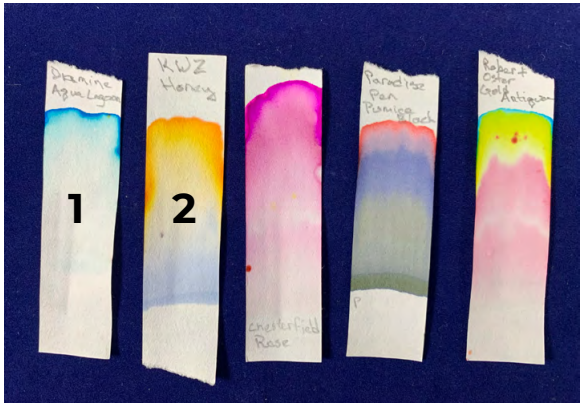


Suspend the filter strip in a small volume of water

The pigment in strips 1 and 2 are the same. This is how you identify that the pen used to write the note belongs to the teacher.

Comparison with the crime scene note

After the chromatography process is complete, ask teams to analyse the colour patterns from all five strips.



The revelation

What do they notice about the chromatography pattern on the crime scene note (strip 1) with the pattern on sample strip 2?

Can they match the ink from this test sample using the teachers pen with the sample from the crime scene note with the teacher's handwriting?

With the evidence gathered, reveal that the teacher is the person who wrote the note, leading to the conclusion they may have committed the cybercrime because the patterns matched the teacher's ink sample.

The memory stick – unmasking the hacker

Instruct the teams to insert the memory stick into a computer's USB port. Ask them to explore the files and folders on the memory stick carefully.

As the groups start exploring the memory stick, they come across files that unmistakably belong to the teacher. For example, photos of the teacher in familiar locations or documents with the teacher's name or school-related materials.

The teacher reveals that the memory stick does indeed belong to them.

They have been caught because they did not take measures to encrypt the files on the memory stick.

With this evidence, along with the crime scene note, it's time to let the school court decide.

The mock trial – time to prepare

The aim of this activity is to promote responsible digital safety and behaviour while engaging in an exciting and memorable mock trial.

Assign each group to create a **crime scene report** based on their investigation and the evidence they have collected.

Each group should carefully analyse the physical and digital evidence, including decoded messages, chromatography experiments and the memory stick. Include photos, notes, sketches and any other relevant information collected.

Mock trial preparation

Introduce the concept of a mock trial to the class and explain the roles involved. **These are prosecutors and defence lawyers, judge and jurors.**

Help each group prepare a presentation of their crime scene report, which they will present during the mock trial. Remind them of the following tips to ensure a fair and engaging trial.

- Equally share speaking parts.
- Speak clearly and confidently while presenting arguments and testimonies.
- Address the judge as 'Your Honour'.

Teacher: please ensure that this is a fictional scenario for the pupils and not a real cybercrime accusation against a teacher.

Time to present the evidence

Begin the mock trial by introducing the case, setting the background and explaining what evidence was found and where. The accused teacher's defence is that they were framed by the real hacker.

Each team should take turns presenting their crime scene report, stating who they think the cyber-hacker is, why they believe so and why they think the teacher was or was not framed for the cybercrime.

The prosecuting and defence lawyers should present their arguments based on the evidence collected. Jurors should carefully listen to all the presentations and evidence to make a fair decision at the end.

Uncovering the master cyber criminal

After all the groups have presented their case, revealing the twist that the teacher was the cyber master criminal all along.

Emphasise the importance of being careful about digital safety and behaviour online and offline.

Encourage open discussions about online interactions, sharing personal information, and the potential risks involved in trusting unknown individuals.

Teacher: the twist in the storyline will make the learning experience exciting and memorable, leaving a lasting impression on the importance of responsible online behaviour.

Decoding answers

WELL DONE GOOD START

YOU WILL NEVER CATCH ME HA,HA!

ONE HUNDRED POUNDS FOR THE MEMORY STICK

Leave a bag of money at school reception on Saturday

Royal Academy of Engineering

The Royal Academy of Engineering is harnessing the power of engineering to build a sustainable society and an inclusive economy that works for everyone.

In collaboration with our Fellows and partners, we're growing talent and developing skills for the future, driving innovation and building global partnerships, and influencing policy and engaging the public.

Together we're working to tackle the greatest challenges of our age.

What we do

Talent & diversity

We're growing talent by training, supporting, mentoring and funding the most talented and creative researchers, innovators and leaders from across the engineering profession.

We're developing skills for the future by identifying the challenges of an ever-changing world and developing the skills and approaches we need to build a resilient and diverse engineering profession.

Innovation

We're driving innovation by investing in some of the country's most creative and exciting engineering ideas and businesses.

We're building global partnerships that bring the world's best engineers from industry, entrepreneurship and academia together to collaborate on creative innovations that address the greatest global challenges of our age.

Policy & engagement

We're influencing policy through the National Engineering Policy Centre – providing independent expert support to policymakers on issues of importance.

We're engaging the public by opening their eyes to the wonders of engineering and inspiring young people to become the next generation of engineers.

Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG

Tel: +44 (0)20 7766 0600
www.raeng.org.uk
Registered charity number 293074