Countdown to Chaos

A guide to delivering the simulated real-time cyber-attack with Key Stage 3 students

Introduction

This resource has been created for you and your students by the Tech Partnership, and we believe that, as the experts in teaching and learning, you will know how to get the most out of it with your students. That said though, we've come up with this short guide to throw a couple of ideas your way about possible ways to deliver it.

Countdown to Chaos is an interactive simulation of a cyber-attack on the UK Power Grid. Your students' job is to analyse the information they are presented with and figure out who is responsible. We have tried to make Countdown to Chaos exciting and realistic using mixed media including video footage, news bulletins and social media messages. These will appear as you work through the resource, and all of these include hints about the possible perpetrator of the cyber-attack. Against the clock, students decide who is responsible – their correct identification of the person behind the attack keeps the lights on. Get the wrong person – and the power grid fails.

No pressure then!

Possible ways to delivery Countdown to Chaos

Countdown to Chaos takes place over four acts. How might you choose to deliver it?

1. In a morning or afternoon, students work through the whole resource.
2. One act per lesson over a series of three or four lessons.
3. As part of an after school club.
4. Using a flipped classroom model.

We have created two pre-teaching lessons you could use to establish the context and a basic understanding of what cyber security is. Some teachers love this idea, while others think it is best to just throw their students straight into it, the surprise element adding to the drama and enjoyment. You know your students best - you decide!

You will find the lesson plans alongside this guide in the Resources section of the Countdown to Chaos course page.

Brought to you by

A flexible resource

The resource has been designed to be flexible. You might decide you want to run the session from the front, with the whole class in small groups. For this, you can project the resource and control it yourself. You will need to click 'move forward' when prompted and you could read out the information on screen to the class, pausing for them to discuss things as you go.

Alternatively, the students could work through the resource independently and at their own speed, perhaps pausing to discuss their thoughts during or after each act.

Details and timings of the action through the Acts

Act One: 30 mins

A film premiere broadcast is hacked by Ambiguous who threaten to shut down the UK power grid but do they have the capacity to carry out such a hack?

Key points in the Act	Tasks/discussion points
Agent Y sets scene	
Film premiere and interview	North Korea and 'The Interview' Sony hack
Ambiguous hack	Anonymous and hacktivism
Email from power grid	Who might be responsible?
Gogogander (Google)	Students sift through info and decide what is important.
Agent Y checks Blabber (Twitter)	How news breaks on Twitter
Blabs	Students sift through info and decide what's important.
Email from grid	What have they learnt? Discussion.
End of Act 1	

Key links to use with the resource

The Interview/Sony hack: http://www.bbc.co.uk/news/entertainment-arts-30512032

Anonymous and hacktivism: http://www.bbc.co.uk/news/technology-20446048

Stories that broke on Twitter first: http://www.techradar.com/news/world-of-tech/internet/10-news-stories-that-broke-on-twitter-first-719532

Key terms:

Cyber crime	Hacking	Controversy
Freedom of speech	Satire	Hacktivist
Price-fixing	Malware	Virus

Act Two: 30 mins

The lights start going out hours before Ambiguous said they would. Could someone else be responsible for the attack on the power grid?

Key points in the Act	Tasks/discussion points
Radio Lumsdon	
Blabber	Twitter as a tool to hold companies to account.
Picshare (Instagram)	Discussion around social media changing how news spreads/bias/trustworthy sources. What might the implications of a nationwide power cut be?
Timegraph	Students analyse info and discuss threat level in their groups.
Blabs	Analyse and note down important info.
Clementine Holmes	What is a malicious insider attack?
End of Act 2	

Key terms:

National outage	Looting	Cyber-terrorism
Culprits	Insider	

Act 3: 30 mins

The UK power grid looks at serious risk of complete blackout. Leaked information and social media seems to be pointing to a number of culprits. Who is to blame?

Key points in the Act	Tasks/discussion points
Agent Y	**Social Engineering** animation; how might people trick their way into buildings?
News/timeline	Student discuss who might be the culprit, how and why.
Blabber #cyberhacks	General discussion: who hacks, how and why?
Fresh Phish	Students share own experiences of receiving phishing emails.
The Truth.com	What is Wikileaks?
End of Act 3	

Key links to use with the resource

The **Social Engineering** animation can be found within the Resources on the course page of Countdown to Chaos alongside three other animations that are available for you to use with your students.

Key terms:

Intruder	Phishing	Monopoly	Firewall
Trojan	Data analyst	Mega-code	

Act 4: 20-30 mins

A crisis meeting at the power grid takes place moments before complete blackout is expected. Can the students work out the culprit and stop them in time?

Key points in the Act	Tasks/discussion points
Agent Y	Groups discuss who they think did it and how.
Skype Call	Students can discuss if they are sticking to their theories and why.
Cluedo	Groups decide by who and how they think the hack was done.
End of Act 4	

Key terms:

Breach	Seized	Resources	Malware
Expertise	Insider	Interrogated	

The solution – what actually happened?

1. Susan Hanrahan's son Billy was hacked by Ambiguous when he turned off the encryption settings on his mum's work laptop to try to win an iPad. Ambiguous were able to access Susan's computer and some HR files including names of employees.
2. Ned was contacted by Montezuma who found out about his gambling problem and agreed to transfer a large sum of money in exchange for inside access to the Grid computer network.
3. Cyber criminals attempted to gain physical access to the systems but were caught.

Teaching ideas

Cyber security is all about assessing risk and trying to avoid attacks. How could these cyber-attacks have been avoided? Discussion points can include:

- Turning off security settings even for a few minutes can let hackers in
- In the end, security attacks usually succeed because of failures with people rather than failures of technology
- Understanding how social engineering can cause usually sensible people to behave in an irresponsible way can prevent cyber attacks
- Sometimes parents really need to know what their children are doing on their computers, particularly when a work computer is used by all family members!

The Flipped Classroom

To deliver the resource as a flipped classroom activity, the students would complete Acts 1-3 for homework with the discussion and research activities taking place in class time.

Act Four would take place during class time with an activity afterwards that explored what actually happened and how the attack took place.

All students can be given access to the resource to use from home through the registration process on the Learning Management System that houses this project, and all other TechFuture Classroom projects. As a teacher, you can monitor your students' progress through the resource and check whether they have worked through it, and how far they went with each act. We can set you up to have administration rights over your own groups of students.