# ENGAGING CYBERSECURITY LESSONS

In this Insider's Guide, **Alan O'Donohoe** gives suggestions for fun and engaging activities to bring cybersecurity lessons to life

**As computing teachers, it is part of our duty to ensure that children grasp the potential risks associated with cybersecurity. But it's also part of our responsibility to ensure they understand some everyday practical actions they can take to reduce the chances of themselves or others being targeted in an attack and to minimise consequent damage. Cybersecurity education, though, presents some challenges:**

- Cybersecurity topics can be dry and dull, making teaching difficult
- The nature of cybersecurity topics means they can sound terrifying
- Teaching cybersecurity tends to be theoretical, as it's not practical to experience an attack
- Students may not perceive themselves as being at risk — they either think they know it all or that they have nothing of value to cybercriminals


## ALAN O'DONOHOE

With 30 years of experience teaching and leading in schools in northern England, Alan leads The Exa Foundation (**exa.foundation**) on a mission to inspire digital makers, support the teaching of computing, and promote the appropriate usage of technology (**@exafoundation**, **@teknoteacher**).


There are, however, opportunities for teachers to make learning about cybersecurity engaging and exciting, while also helping students understand the real-world implications of poor online security. In this article, I provide practical examples of activities that you can use to make the teaching of cybersecurity more interesting for your young students. The brute-force attack activity could easily last a full lesson, but the others work better as a smaller part of a lesson, to test and develop understanding.

Teachers can adapt these activities to work with learners of different ages. For example, I've used the first activity with children as young as seven, and have used all these activities with parents and staff members as part of training sessions. You may use them as described first before modifying to suit your preferred teaching style and particular audience. (HW)

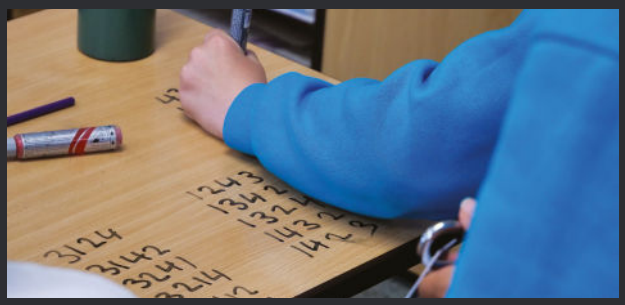
## BRUTE-FORCE ATTACK

In this activity, through the use of combination padlocks, learners are able to model the principles of a brute-force attack and apply these to password security. I begin by telling the class that I will be distributing ten padlocks around the room and the goal is for them to work together in groups to unlock them. However, before anyone is allowed to touch them, we will discuss strategies they can use.

A brute-force attack is a method cybercriminals use to guess a password by trying every possible combination until the correct one is found. Typically, this is performed by an algorithm capable of guessing thousands of combinations every second. Encourage the students to think about how this concept applies to the padlocks in front of them.

I ask the class to calculate how many possible combinations a four-dial padlock has, and if they were able to test one every second, the maximum amount of time it would take (2 hours, 46 minutes, 40 seconds!). Humans can get tired; they need breaks, make mistakes, and are lazy, so we discuss strategies they could use to reduce this amount of time. Students may ask the teacher questions to reduce the number of possible combinations. I tell them I will never reveal the full code, but I may accidentally give away hints to each team (for example, 'Two of those numbers are correct, but in a different order', or 'No numbers appear more than once'). I remind teams to collaborate by exchanging what they know with other teams to reduce the time required, and stress the importance of keeping and sharing a record of the combinations they have already tried.

It's difficult to predict how long it will take for students to successfully unlock the padlocks. I use the same code for all padlocks. This creates another learning opportunity around the convenience of having only one password versus the risks. It's important to plan for some reflection time at the end to discuss the lessons learnt, the importance of using strong passwords that are difficult to guess to prevent brute-force attacks, and the extra security that multifactor authentication offers.



Children work collaboratively to guess the code for a combination lock using a brute-force method

## WHAT'S IN THE BAG?

**Recommended amount of time:** flexible, from 2 minutes up to 20 minutes, depending on the time available. Each phrase selected requires only a minute or two, so it could be used at the end of a lesson with whatever time is available.

This engaging activity is called 'What's in the Bag?' It can develop students' confidence with technical vocabulary while also encouraging them to think critically about cybersecurity risks and strategies in a light-hearted way.

I prepare a bag containing a set of cards, each with a technical term on it connected to cybersecurity. The technical terms represent a mix of threats (potential cyber risks) and protections (security tools and strategies that can be used to reduce cyberattacks). To add a bit of fun, you can also include a few terms that have no obvious connection to cybersecurity. I have used breeds of cats such as Russian Blue, Persian, Ragdoll, and so on. In my experience, students have enjoyed these surprise elements of fun, and there have even been occasions when students have tried to convince me that Russian Blue is a kind of virus or a hacking group!

To begin the activity, the teacher reaches deep into the bag, adding an element of drama and surprise, as they select a phrase and read it aloud. Student players have to respond quickly to correctly identify the phrase and categorise it as threat, protection, or cat (or other distractor). It also works well when students are organised into teams that compete against each other, with a point awarded when teams correctly identify whether the term is a threat or a protection. The teacher may select individual team members in turn to respond initially, then allow the team to discuss the details before scoring additional points for an explanation. If teams correctly identify that the term is a distractor, they score a bonus of three points. After correct identification, the teacher may ask teams, for additional points, to explain what the phrase means and how it relates to cybersecurity. For example, if the phrase 'phishing' is selected, the students would need to identify it as a threat and explain what a phishing attack is, the methods used by perpetrators to conduct such an attack, how a potential victim can spot a phishing scam, and steps they could take to protect themselves against it.


Prepare a bag containing a set of technical terms connected to cybersecurity. Can you spot the breed of cat?

Occasionally, I filter out some terms before starting the activity so that the remaining collection reflects the ability of the teaching group. The set I prepare includes a combination of complex technical terms and more obvious terms, so that there's something for everyone.

## PACKET EXCHANGE

**Recommended amount of time:** 20–30 minutes. This activity is worth repeating so that students get the hang of it.

The teacher prepares a set of double-sided cards, with one side featuring a phrase related to cybersecurity and the other featuring a comprehensive definition of that phrase.

Students are then paired up and take turns asking their partner to define the phrase on their card. If the partner being quizzed needs help, the questioner can use the definition on the reverse of the card to provide support in answering the question. However, the questioner needs to judge how subtle or strong the help they provide should be, depending on how successfully the quizzed partner is able to define their phrase. There is skill in providing just enough support so that the person answering is able to arrive at the definition themselves without too many prompts. After each student has quizzed their partner, they swap cards with each other, or find a new partner, and repeat the activity. This allows students to learn from each other and reinforce their understanding of key cybersecurity concepts.

From experience, I've found that students have enjoyed learning about cybersecurity in this way because it encourages collaboration and support, and develops understanding in a non-threatening way. By working with their peers, students are able to reinforce their understanding of key concepts and develop the skills they need to stay safe and secure online.

By working with their peers, students cam reinforce their understanding of key concepts


There are plenty of opportunities for teachers to make learning about cybersecurity engaging and exciting

## CYBERSECURITY SONGS

Through my work with The Exa Foundation, I've been visiting primary and secondary schools across England to help school communities (not just children) develop their understanding of cybersecurity risks. Visiting different learning settings helps me develop different approaches all the time as I seek to find new and engaging ways of presenting the content. One of my latest endeavours has been to rewrite the lyrics of popular songs, adapting the messages to a cybersecurity theme. I'm fully aware that I have a terrible singing voice, and the lyrics still need some work. However, I have noticed that the children respond very positively!

I ask the class to list all the cyberthreats or protection strategies they can identify while I perform the song, then we review them to see how many they spotted correctly. Finally, I'll share the lyrics on screen, and some classes like to join in the song for a second rendition. *Attack, Survived* is one of my latest examples and I perform it to an instrumental/karaoke version of Gloria Gaynor's *I Will Survive*. If you'd like to know more about the other songs, get in touch!

**ATTACK, SURVIVED**

**At first, I never knew, till the day you tried**
**To brute force my account, then my network died**
**Soon came the phishing scams, they all strung me along**
**They did me wrong, I should have made my passwords strong**

**Then a DDoS attack, emoji evil face**
**Found your digital footprints after running a network trace**
**I should have changed those stupid passwords, used multifactor too**
**If I'd known about your cyber tricks, I'd have never trusted you**

**CHORUS**
**Log off now, go, forever more**
**You're locked out now, I've shut down that back door**
**Weren't you the one who tried to cause a data breach?**
**Now you've been rumbled, it's time you said goodbye**

**Next time you try, attack denied**
**Automated backup strategies will help protect my files**
**I've got all my firewalls on, all my data's encrypted strong,**
**Attack survived, attack survived**

**Port scans helped identify potential risks**
**Closed them down, reduced exposure to your hacker tricks**
**I spent oh so many nights building my network defence**
**I used to be clueless, but now I've developed cyber sense**

**And you see me, somebody new**
**I'm not that careless little n00b who once trusted you**
**You thought zero day made me a target, then you failed to see**
**I quickly patched my software to reduce vulnerabilities**

**CHORUS**
**Go on then try, attack denied**
**Regular antivirus updates, protect all my drives**
**I've got auto updates on, I've made all my passwords strong,**
**Attack survived, attack survived**