Your Activity

Understanding cybercrime and how to stay safe online.

You have learned about the most widespread cybersecurity threats and how to protect against them. Now, it’s time to put your knowledge to the test with a few quizzes and discussions.

Time for a quiz!

Click here to access the Understanding cybercrime and how to stay safe online presentation.

QUICKLINE
Broadband built for you

Activity 1

Can you guess the top 5 most commonly used unsafe passwords worldwide?

Type 1 letter/number per box to make your guess.

Once you've completed all 5 passwords go to the next page to reveal the answers.

1 *Hint: A secret word.*

P A S S w o r d

2 *Hint: Counting.*

1 2 3 4 5 6

3 *Hint: Counting, but longer!*

1 2 3 4 5 6 7 8 9

4 *Hint: When you're connecting to a hotel WiFi, you connect as a _____.*

g U e s t

5 *Hint: The start of your keyboard.*

q w e R t y

Activity 1

Can you guess the top 5 most commonly used unsafe passwords worldwide?

Reveal answers

→

Activity 2

This activity requires you to:

1. Pick four types of cybercrime out of the list provided.

2. Rank the types of cybercrime selected in order of severity, from ‘not at all serious’ to ‘very serious’, based on your own perception and experience.

Be prepared to discuss your ranking as you fill out your ranking!

Of course, all types of crime are serious and punishable by law. But here, we want you to think about how you would feel if you were the victim, as well as how and how severely other people could be affected by these cybercrimes.

not at all serious

1

2

3

4

very serious

Learn more:
Cybercrime in the news.

Ransomware

Cyberespionage

Online identity theft

DoS attack

Cyberstalking

Phishing

Ransomware

According to a 2023 press release by GOV.UK:

> The ransomware strains known as Conti and Ryuk affected **149 UK individuals and businesses.** The ransomware was responsible for extricating at least an estimated **£27 million.** There were 104 UK victims of the Conti strain who paid approximately £10 million and 45 victims of the Ryuk strain who paid approximately £17 million.
>
> Conti was behind **attacks that targeted hospitals, schools, businesses and local authorities,** including the Scottish Environment Protection Agency.
>
> Conti was one of the first cyber crime groups to **back Russia's war in Ukraine,** voicing their support for the Kremlin within 24 hours of the invasion.
>
> Although the ransomware group responsible for Conti disbanded in May 2022, reporting suggests members of the group continue to be involved in some of the most notorious new ransomware strains that dominate and threaten UK security.

⌂ Activity 2

DoS attack →

DoS attack

According to a 2021 **BBC article:**

> An unprecedented and coordinated DoS attack has struck multiple UK-based providers of voice over internet protocol (VoIP) services, used by many companies and more notably by **the NHS and police.**
>
> DoS attacks work by flooding a website or online service with internet traffic in an attempt to throw it offline or otherwise make it inaccessible, in an effort to extort.

Activity 2

Online identity theft →

Online identity theft

According to a 2022 article by **TechHQ:**

> In the UK, new research has shown that data breaches driven by identity theft, since 2013, are costing the country nearly **£4 billion every year,** and a total of over 140 million files have been compromised in the same period, consisting of **documents, passports and bank statements.**
>
> Credit card fraud has also surged, with the UK called the "credit card fraud capital of Europe" by the Social Market Foundation. Brits also fall victim to scammers more than other European countries.

Activity 2

Phishing →

Phishing

According to a 2022 article by **The Guardian:**

> More than **£1.3bn was stolen** by con artists last year, figures reveal, with authorised push payment fraud (APP), where victims are tricked into making a payment. Nearly 40% of APP fraud losses were due to impersonation scams, where criminals pretend to be from a trusted contact to trick victims into moving their money, with an estimated £214.8m stolen using this method in total.
>
> Criminals impersonated organisations such as the NHS, banks and government departments via phone calls, texts, emails, fake websites and social media posts to trick people into handing over their personal and financial information that was then used to convince account holders to make a payment.

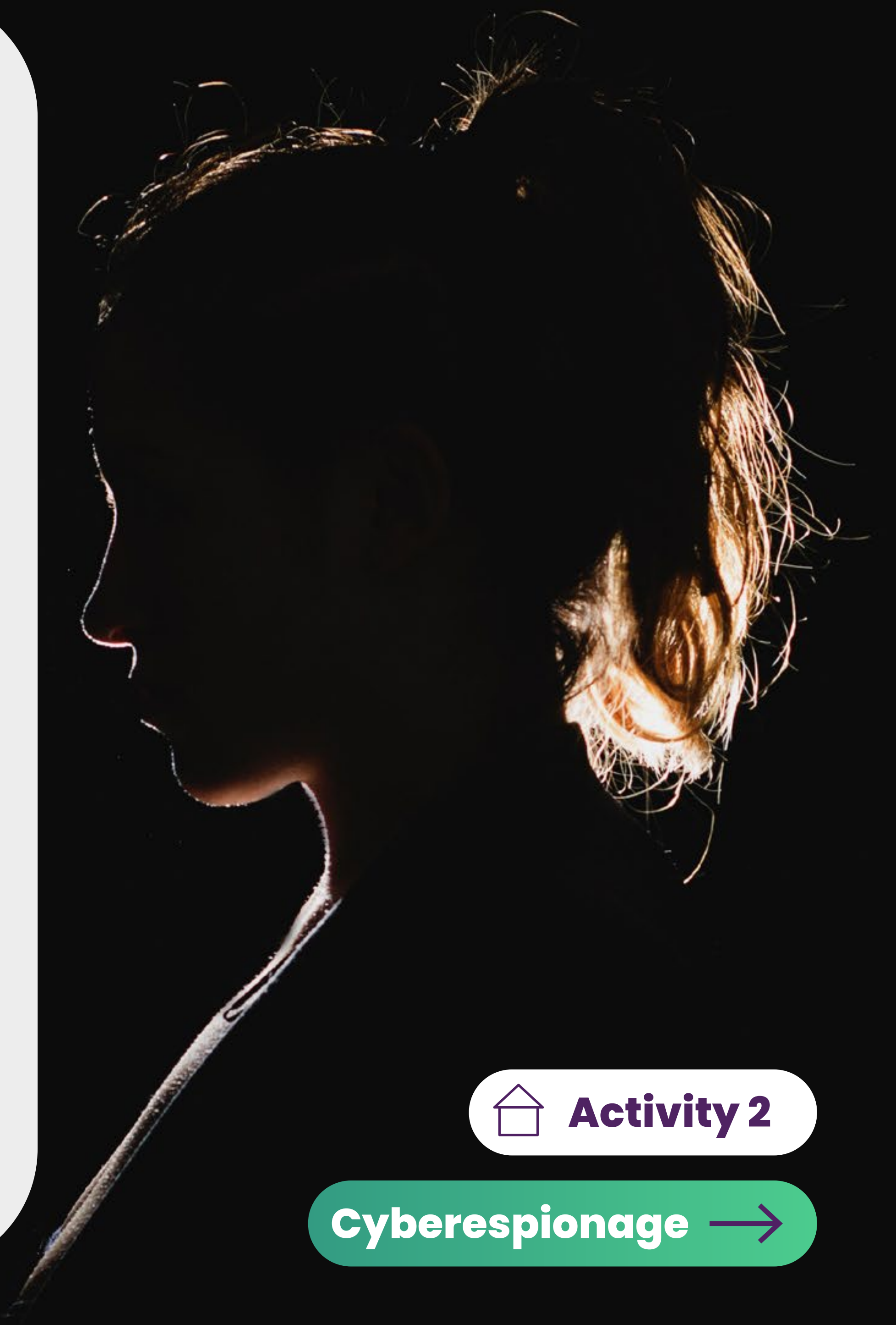
Activity 2

Cyberstalking →

Cyberstalking

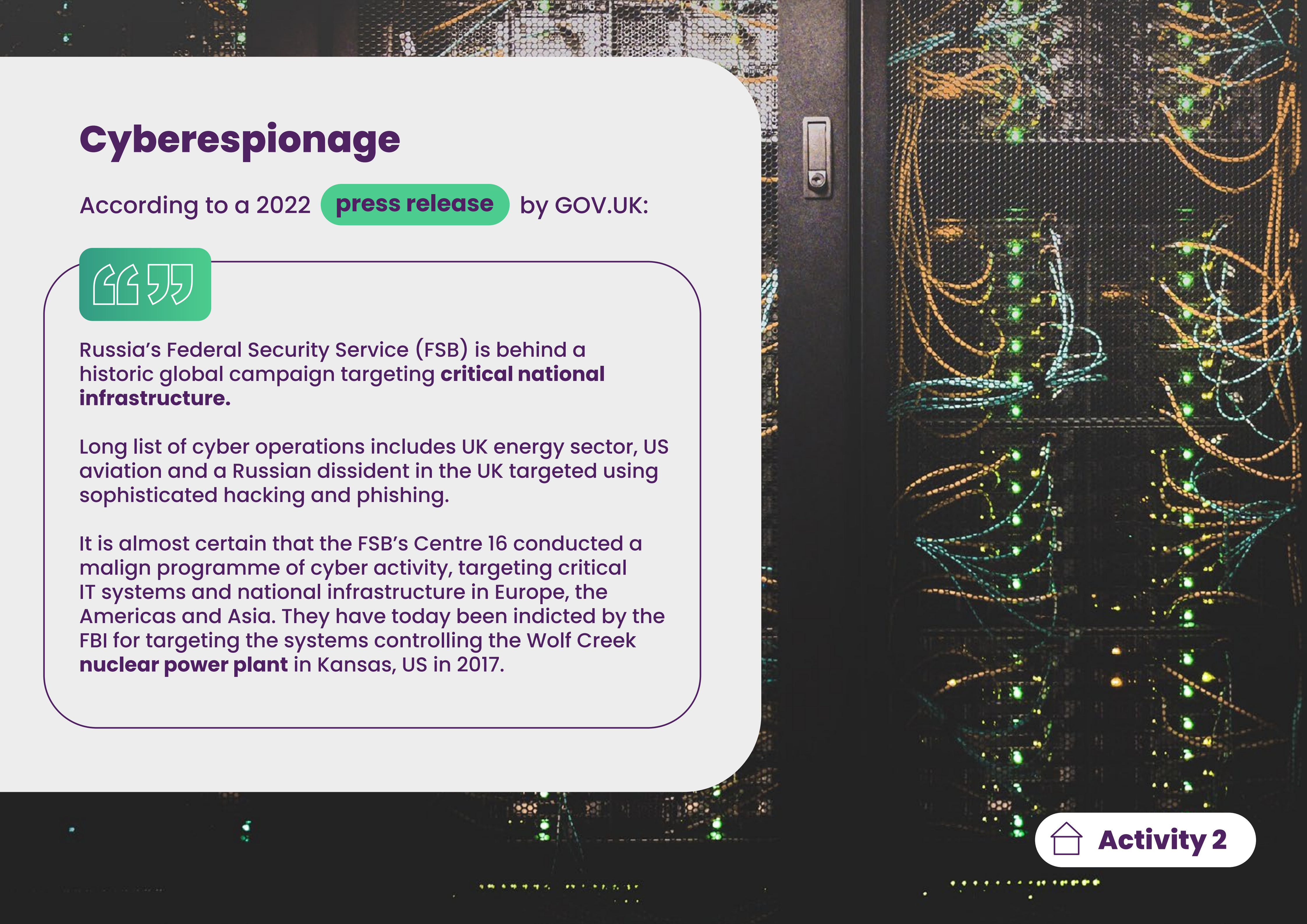
According to a 2022 article by **The Guardian:**

> The conversations always started the same way. A woman would get a message from a social media user. It would say: “Can I tell you a secret?”
>
> The messenger would also claim to have information about the woman’s life. The victim’s partner was cheating on her; a friend was talking behind her back. If the woman blocked the anonymous messenger, another appeared. If the woman stopped responding, she would get incessant calls from someone breathing down the phone.
>
> This stalking could go on for years.
>
> **Victims lost friends, family members, relationships and professional opportunities.** One terrified victim slept with a baseball bat in her hand. Another kept a samurai sword beside her bed. Some were diagnosed with depression and anxiety and needed medication.



Activity 2

Cyberespionage →



Cyberespionage

According to a 2022 **press release** by GOV.UK:

> Russia’s Federal Security Service (FSB) is behind a historic global campaign targeting **critical national infrastructure.**
>
> Long list of cyber operations includes UK energy sector, US aviation and a Russian dissident in the UK targeted using sophisticated hacking and phishing.
>
> It is almost certain that the FSB’s Centre 16 conducted a malign programme of cyber activity, targeting critical IT systems and national infrastructure in Europe, the Americas and Asia. They have today been indicted by the FBI for targeting the systems controlling the Wolf Creek **nuclear power plant** in Kansas, US in 2017.

Activity 2