# Edinburgh schools reopen on Saturday after phishing attack locks thousands out of exam resources



Thousands of pupils in Edinburgh faced a disruption this past weekend as they were called upon to reset their IT network passwords due to a phishing attack that had locked them out of crucial learning materials. The incident unfolded urgently on the Friday before exams, prompting the City of Edinburgh Council to open all secondary schools on Saturday, enabling approximately 2,500 students to regain access to their online study resources.

The cyber attack was identified when a staff member reported “unusual and suspicious” activity across the schools' IT network. In response, the council took a precautionary measure by initiating a password reset for all users, effectively locking staff and students out until they established new credentials. Education convener James Dalgleish expressed gratitude to school staff for their swift response, noting that their vigilance helped mitigate potential disruptions to students’ exam preparations. "My thanks once again to our colleagues for their quick thinking and vigilance, without which this could have been far worse," he stated.

As the incident unfolded, the Scottish Government affirmed that no data had been compromised, and the situation was being closely monitored. A spokeswoman for the government noted that the City of Edinburgh Council was receiving support from the Scottish Cyber Co-ordination Centre. The ministers were also reassured about the impact on exam arrangements, signalling a commitment to uphold the integrity of the educational experience during such crises.

This incident in Edinburgh is not an isolated case, reflecting a broader trend of increasing cyber threats in educational institutions across the UK. According to the Cyber Security Breaches Survey 2024, a staggering 92% of primary schools and 89% of secondary schools reported experiencing phishing attacks within the last year. This alarming statistic underscores the pressing need for robust cybersecurity measures within the sector, as educational institutions often handle sensitive data and thus become prime targets for cybercriminals.

The situation raises pertinent questions about the overall resilience of educational networks against cyber threats. Recent events, such as a major security breach in Education Scotland’s digital learning platform Glow, which necessitated a password reset across the board due to potential safeguarding risks, highlight the fragility of online educational systems. In that incident, students were inadvertently encouraged to share credentials, emphasising the crucial nature of cybersecurity education and protective policies.

Adding to the narrative of vulnerability, the incident in Edinburgh mirrors a recent ransomware attack on schools, including the Harris Federation in London, that rendered 37,000 pupils unable to access their email due to encrypted data. The National Cyber Security Centre has issued multiple alerts regarding rising attacks on educational facilities, advocating for heightened security measures and awareness.

In light of these threats, educational bodies are making strides to bolster cybersecurity awareness. Initiatives like the Cyber Security Escape Room, which engages students in simulated cybersecurity challenges, aim to better prepare young individuals for the realities of digital threats. This proactive educational approach reflects a broader understanding of the importance of integrating cybersecurity into the curriculum, ensuring that students are not only recipients of education but also equipped to navigate and secure their digital environments.

The response in Edinburgh showcases a collective effort to overcome cyber challenges while maintaining educational integrity, reflecting both the urgency of the current landscape and the resilience of the community. As students prepare for critical exams, the ongoing commitment to enhancing cyber resilience remains a priority for all stakeholders involved in their education.

Such incidents reinforce the urgency for all educational institutions to prioritise cybersecurity, ensuring that they not only react swiftly to threats but also build extensive preventative strategies to safeguard the future of learning.

### Reference Map

1. Paragraphs 1-4
2. Paragraphs 5-6
3. Paragraph 7
4. Paragraph 8
5. Paragraph 9
6. Paragraphs 10-11

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.independent.co.uk/tech/scottish-government-edinburgh-schools-police-scotland-uk-government-b2748563.html> - Please view link - unable to able to access data
2. <https://www.thecourier.co.uk/fp/education/schools/676331/education-scotland-order-hard-reset-on-school-social-networking-app-following-major-security-breach/> - Education Scotland ordered a hard reset of all passwords across its national digital learning platform, Glow, following a major security breach. The breach occurred when children were encouraged to share their credentials with parents, potentially allowing unauthorized access to applications like Yammer, a social networking tool for students. The incident raised concerns about safeguarding and data privacy, prompting Education Scotland to refresh existing passwords and provide guidance to local authorities on appropriate actions.
3. <https://www.heraldscotland.com/news/13416078.thousands-email-addresses-stolen-cyber-attack-edinburgh-council/> - A cyber attack on Edinburgh City Council's computer system resulted in the theft of personal details, including email addresses, of over 13,000 individuals. The council swiftly addressed the issue, assuring that no services were affected. Affected individuals were contacted and advised to change passwords used to access the council's website. The Information Commissioner's Office was informed, and preventive measures were implemented by the web service providers to enhance security.
4. <https://www.bbc.co.uk/news/technology-56569873> - A ransomware attack on multiple schools, including the Harris Federation in London, left 37,000 pupils unable to access their email. The Harris Federation temporarily disabled email systems while addressing the cyber-attack, during which data was encrypted and hidden by attackers. The National Cyber Security Centre (NCSC) had previously warned that hackers were targeting schools, highlighting the increasing threat to educational institutions.
5. <https://www.llex.hk/news/other/parents-conned-out-of-large-sums-in-cyber-attack-on-fettes-college/ar-BB1pmfnQ> - Fettes College in Edinburgh, known as the 'Eton of the North', was targeted by hackers in May 2024. Criminals sought to defraud families by illegally obtaining their details. A 'handful' of families were conned out of substantial sums. The school took immediate steps to resolve the situation, involving police and IT experts, and launched a full investigation. Parents were advised to be alert to any unusual communication from the school.
6. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/education-institutions-annex> - The UK's Cyber Security Breaches Survey 2024 revealed that 92% of primary schools and 89% of secondary schools experienced phishing attacks in the last 12 months. Further education colleges reported a 97% rate, and higher education institutions had a 100% rate. The survey highlights the prevalence of cyber threats in educational settings and underscores the need for robust cybersecurity measures.
7. <https://siliconscotland.com/cyber-security-escape-room-launched-for-edinburgh-schools/> - Stellar Omada, in partnership with the Heart of Midlothian Innovation Centre, launched a Cyber Security Escape Room initiative for Edinburgh schools in December 2024. The program aimed to raise awareness about online safety, with over 200 pupils from secondary schools participating. Small groups of pupils worked together to tackle simulated cybersecurity scenarios with expert guidance, emphasizing the importance of cybersecurity education.