# Edinburgh pupils locked out of revision platforms after spear-phishing cyber attack



Pupils in Edinburgh recently faced significant disruption to their exam preparations following a cyber attack that targeted the city’s education network. In a precautionary measure, the council reset all student passwords after detecting a suspicious spear-phishing attempt, which sought to impersonate a trusted source. This decisive action meant that students were cut off from critical learning resources just as they were gearing up for key examinations.

Councillor James Dalgleish, who oversees education and children's services in the city, reported that staff quickly identified the "unusual and suspicious activity" on the IT network. "As a result, we took the precautionary decision to immediately reset passwords for all users across our education service," he stated. While this step was necessary to protect the integrity of the network, it left many students, including those scheduled to sit exams soon after, unable to access vital revision materials. This included access to Microsoft Teams, a platform heavily relied upon by students for their studies.

The council acknowledged the inconvenience caused, especially for those with impending exams, such as the Higher maths exam scheduled for the following Monday. To mitigate some of the disruption, pupils were granted access to schools over the weekend, where staff issued them new passwords. Additionally, the council established an online help page to aid students in navigating the situation.

Students expressed their frustrations over the disruption. Jack, 18, described the situation as a "nightmare," highlighting how critical digital resources are for effective revision. His sister Libby, 16, remarked on the added stress for those living further from school, compounded by the limited time available for last-minute preparations.

This incident follows a similar attack on West Lothian schools just days earlier, which had prompted the local authority to enact contingency measures to ensure its schools remained operational. Thankfully, initial reports indicated no personal or sensitive data had been compromised in either case, as both Edinburgh and West Lothian councils collaborated with security agencies and local law enforcement to enhance their IT protections.

Cybersecurity experts note that spear-phishing attacks, characterized by their meticulous targeting and deceptive communications, are increasingly common within educational sectors. Unlike traditional phishing attempts, which cast a wide net, spear-phishing messages are often tailored to convince the recipient of their authenticity, leading to potential breaches that can have far-reaching consequences.

This is not the first time Edinburgh City Council has faced cybersecurity challenges. In June 2015, the council became the victim of a cyber attack that resulted in the theft of over 13,000 email addresses. At that time, the council took immediate action by informing affected individuals and updating security measures to mitigate future risks.

As Edinburgh's education department works to return to normalcy, the Scottish Qualifications Authority (SQA) has been briefed on the events, and pupils are encouraged to voice any concerns with their teachers. The council aims to have all systems fully operational by Monday, allowing students to resume their studies with some assurance of the continuity of their educational resources.

This recent wave of cyber incidents highlights the pressing need for robust cybersecurity measures across public sector institutions, particularly within vulnerable sectors like education. Authorities are tasked with not only defending against these attacks but also ensuring that the educational process remains uninterrupted in the face of such threats.

### Reference Map

1. Paragraph 1 - Sources 1, 4, 5
2. Paragraph 2 - Sources 1, 4
3. Paragraph 3 - Sources 1, 5
4. Paragraph 4 - Sources 1, 4
5. Paragraph 5 - Sources 1, 6
6. Paragraph 6 - Sources 2, 3
7. Paragraph 7 - Sources 1, 6
8. Paragraph 8 - Sources 7, 1

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

## Bibliography

1. <https://www.aol.com/news/pupil-passwords-reset-council-cyber-211516332.html> - Please view link - unable to able to access data
2. <https://www.bbc.com/news/uk-scotland-edinburgh-east-fife-33425853> - In June 2015, Edinburgh City Council experienced a cyber attack that resulted in the theft of over 13,000 email addresses from its database. The breach occurred when the council's website service provider was targeted by hackers. The council assured that no other personal details were accessed and warned of potential increases in spam or phishing emails. The incident was reported to the Information Commissioner and the UK Government's Computer Emergency Response Team, with additional security measures implemented.
3. <https://www.heraldscotland.com/news/13416078.thousands-email-addresses-stolen-cyber-attack-edinburgh-council/> - In June 2015, a malicious cyber attack on Edinburgh City Council's website led to the theft of over 13,000 email addresses. The council promptly contacted affected individuals, advising them to change any passwords used to access the council's website. The Information Commissioner's Office was informed, and preventive measures were taken by the web service providers. The council emphasized the importance of ongoing website security and continued collaboration with service providers to address associated risks.
4. <https://www.independent.co.uk/tech/schools-edinburgh-b2748326.html> - In May 2025, Edinburgh schools were targeted by a phishing attack that locked students out of online learning materials. The attack was detected when staff noticed unusual activity on the city's schools and early years IT network. As a precaution, the council reset passwords for all users, leaving staff and students unable to log into the network until they reset their passwords. Students preparing for exams were given priority support to regain access to personal revision materials.
5. <https://www.standard.co.uk/news/tech/schools-edinburgh-students-b1226965.html> - In May 2025, a phishing attack on Edinburgh schools resulted in students being locked out of online learning materials. The attack was detected when staff noticed unusual activity on the city's schools and early years IT network. The council reset passwords for all users as a precautionary measure, leaving staff and students unable to log into the network until they reset their passwords. Students currently sitting exams were given priority support to reset their passwords and regain access to personal revision materials.
6. <https://www.edinburghnews.scotsman.com/news/criminal-investigation-into-cyberattack-affecting-86-west-lothian-schools-continues-5118769> - In May 2025, West Lothian Council was alerted to a ransomware attack targeting its education network, affecting all 86 schools in the area. The council worked with Police Scotland and the Scottish Government to resolve the matter, with initial assessments showing no personal or sensitive data had been accessed. All schools remained open, and exams were not affected. The council emphasized the importance of ongoing security measures and continued collaboration with external agencies to address associated risks.
7. <https://www.edinburghnews.scotsman.com/news/edinburgh-schools-cyber-attack-city-schools-targeted-in-phishing-scam-ahead-of-exams-5122134> - In May 2025, Edinburgh schools were targeted by a phishing scam ahead of exams, leading to the resetting of passwords across the council's schools and early years network. The council issued communications to all parents, carers, and schools to advise of the phishing attempt and explain the actions taken to ensure IT networks remained secure. Students preparing for exams were given priority support to reset their passwords and regain access to personal revision materials.