# Edinburgh schools locked out of online resources after phishing attack amid exam period



Schools in Edinburgh are grappling with the fallout from a recent phishing attack that has left students locked out of essential online learning resources. The incident came to light on a Friday afternoon when a staff member detected "unusual and suspicious" activity on the city's schools and early years IT network. In response, the local council decided to reset passwords for all users, which has hindered access for both students and staff until they can reset their credentials when they return to school.

For students currently sitting exams, the council has implemented "priority support" measures, allowing them to regain access to their personal revision materials. Advising that students can visit their schools on Saturday to obtain new passwords, the council has aimed to minimise disruption during this critical academic period. Fortunately, there has been reassurance that no personal data was compromised during this breach, alleviating some concerns about the potential fallout of such cyber incidents.

Councillor James Dalgleish, who leads on education within the council, commented on the situation, acknowledging the significant impact of the attack particularly on exam-preparing students. He mentioned, “This was a difficult but necessary decision to ensure our networks remain secure and protected,” emphasizing the district’s commitment to student safety and data security. The council has also established a dedicated webpage to provide ongoing updates regarding the situation, along with alternative study resources to support affected students.

This incident highlights a growing concern regarding cybersecurity in educational institutions, especially in light of data from a government report indicating that over a third of schools in England experienced a cyber incident in the 2023/24 academic year, with phishing attacks accounting for a substantial portion. The North-West region notably reported the highest number of such incidents, underscoring the urgent need for enhanced cybersecurity protocols across educational settings.

This attack is not an isolated event; earlier this year, Edinburgh City Council fell victim to a separate cyber attack, which resulted in the theft of personal details, including email addresses, of over 13,000 individuals. Such incidents reinforce the importance of robust cybersecurity measures and the need for ongoing vigilance from both educational institutions and individuals. In the broader context of rising cyber threats, a coordinated response among local authorities and schools becomes paramount to protect sensitive information and mitigate future risks.

Moreover, while Edinburgh schools are currently taking steps to address this immediate incident, a wave of malicious emails directed at schools in Glasgow and other areas illustrates a wider regional issue. Police Scotland is actively investigating these threats, signalling the seriousness with which authorities are treating the escalation of cybercrime in educational environments.

As the landscape of education increasingly relies on digital platforms, the narrative surrounding cybersecurity must evolve. Institutions must prioritise the protection of their networks and the sensitive data they hold, while also educating students and families on safeguarding their information online. The ongoing challenges faced by schools in responding to such threats raise critical questions about the adequacy of existing protections and the necessity of implementing more stringent cybersecurity frameworks.

In this era of heightened digital engagement, the resilience of schools against cyber threats will not only determine the stability of their educational delivery but also shape the cybersecurity landscape for future generations. As Edinburgh schools navigate this current crisis, the insights gleaned will be vital in fortifying their defences against the evolving nature of cyber threats.

### Reference Map

1. Lead Article
2. Summary (2)
3. Summary (3)
4. Summary (6)
5. Summary (4)
6. Summary (3)

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

## Bibliography

1. <https://www.independent.co.uk/tech/schools-edinburgh-b2748326.html> - Please view link - unable to able to access data
2. <https://www.independent.co.uk/tech/schools-edinburgh-b2748326.html> - Edinburgh schools experienced a phishing attack that led to students being locked out of online learning materials. The attack was identified when staff noticed unusual activity on the city's IT network. As a precaution, the council reset passwords for all users, requiring staff and students to reset their passwords upon returning to school. Priority support was provided to students taking exams to regain access to revision materials. The council confirmed that no data was compromised during the attack.
3. <https://www.heraldscotland.com/news/13416078.thousands-email-addresses-stolen-cyber-attack-edinburgh-council/> - A cyber attack on Edinburgh City Council's website resulted in the theft of personal details, including email addresses, of over 13,000 individuals. The council responded promptly, informing affected individuals and advising them to change any passwords used to access the council's website. The Information Commissioner's Office was notified, and preventive measures were implemented by the web service providers. The council emphasized the importance of website security and continued collaboration with service providers to address associated risks. ([heraldscotland.com](https://www.heraldscotland.com/news/13416078.thousands-email-addresses-stolen-cyber-attack-edinburgh-council/?utm_source=openai))
4. <https://www.heraldscotland.com/news/24691580.number-scottish-schools-targeted-malicious-messages/> - Police Scotland initiated an investigation after multiple schools across Glasgow and the west of Scotland received malicious emails. The emails were sent to an unspecified number of schools in Glasgow, South Lanarkshire, East Renfrewshire, and East Dunbartonshire. The police responded promptly, and inquiries were conducted in conjunction with local authorities to trace those responsible. The nature of the emails and their content were not disclosed, but the police treated the matter seriously. ([heraldscotland.com](https://www.heraldscotland.com/news/24691580.number-scottish-schools-targeted-malicious-messages/?utm_source=openai))
5. <https://www.telegraph.co.uk/news/2024/07/02/hackers-private-school-place-fettes-college-scotland/> - Fettes College in Edinburgh, a prestigious boarding school, was targeted by hackers in May 2024. Criminals obtained details of wealthy parents seeking to enroll their children and sent fraudulent emails claiming that an additional payment was required to secure a place. A 'handful' of families fell victim to the scam, involving substantial sums of money. The school took immediate action, reported the incident to the appropriate authorities, and advised parents to be vigilant against unusual communications. ([telegraph.co.uk](https://www.telegraph.co.uk/news/2024/07/02/hackers-private-school-place-fettes-college-scotland/?utm_source=openai))
6. <https://www.infosecurity-magazine.com/news/cyber-attacks-third-english-schools/> - A government report revealed that over a third (34%) of English schools and colleges experienced a cyber incident in the 2023/24 academic year. Among these incidents, 23% were phishing attacks. The North-West region was the most affected, with 40% of schools reporting cyber incidents. The report highlighted the significant impact of such attacks, including disruptions to teaching and learning, and emphasized the need for enhanced cybersecurity measures in educational institutions. ([infosecurity-magazine.com](https://www.infosecurity-magazine.com/news/cyber-attacks-third-english-schools/?utm_source=openai))
7. <https://www.edinburghnews.scotsman.com/news/crime/edinburgh-parents-warned-to-check-childrens-phones-after-schoolgirl-8-is-victim-of-sextortion-5008870> - Parents in Edinburgh were warned to monitor their children's phones after an eight-year-old girl from Gilmerton Primary School became a victim of sextortion. A person impersonating pupils on Snapchat targeted multiple students, leading to a police investigation. The school's headteacher urged parents to check all children's social media accounts, report suspicious activity to Police Scotland, and emphasized the importance of online safety. ([edinburghnews.scotsman.com](https://www.edinburghnews.scotsman.com/news/crime/edinburgh-parents-warned-to-check-childrens-phones-after-schoolgirl-8-is-victim-of-sextortion-5008870?utm_source=openai))