# Scotland’s schools face rising threats as phishing exploits lock out students



In recent weeks, schools across Scotland have become increasingly vulnerable to cyber-attacks, highlighting a critical gap in cybersecurity awareness among young users. This trend has been starkly illustrated by incidents involving the City of Edinburgh Council and West Lothian Council, where phishing exploits have locked students out of online learning resources. The severity of these attacks is underscored by the fact that they forced authorities to implement immediate password resets for all users—staff and students alike—raising significant concerns about how well young people are equipped to handle such threats.

Dr Suzanne Prior, a cybersecurity expert at Abertay University, has been at the forefront of examining these vulnerabilities. She points out that there is a widespread misconception that children are inherently safer online due to their familiarity with technology. In reality, Dr Prior argues, this perceived competence may contribute to their increased risk. Her research suggests that, beneath a surface understanding of technical terminology like "encryption" and "firewalls," many young people lack the deep comprehension necessary to navigate potential online hazards effectively. This disconnect can make them particularly susceptible to sophisticated phishing schemes designed to trick them into revealing sensitive information.

Phishing, the act of deceiving people into disclosing personal information, is becoming a prevalent threat in educational settings. Recent data reveals a dramatic increase in these attacks, particularly against K-12 institutions. A report indicated that the number of affected districts doubled from 2022 to 2023, with 108 districts suffering incidents. The ramifications of such cyber intrusions can be severe: from operational disruptions to financial losses and potential breaches of sensitive personal information. Notably, schools often possess a wealth of data—from names and birth dates to academic records—making them prime targets for cybercriminals.

What exacerbates the vulnerability is the environment in which young people are learning. Schools have become heavily reliant on technology, a shift accelerated by the COVID-19 pandemic. Dr Prior reminds us that while the infrastructure is evolving, the most significant weak point remains the users—students and staff who may have limited experience and training in cybersecurity. Teachers, despite some having undergone basic cybersecurity training, do not typically have the extensive knowledge required to effectively safeguard against these threats.

Furthermore, phishing attacks can be broadly categorised into two types: mass attacks, which involve indiscriminate targeting of numerous individuals, and spear phishing, which targets specific individuals with tailored messages. The implications of these attacks extend beyond immediate security concerns; they can severely erode trust among students, parents, and staff, leading to long-lasting reputational damage for educational institutions.

In light of these challenges, Dr Prior emphasises the necessity of ongoing education about online safety. Children must not only be taught about potential dangers but also how to remain vigilant in their everyday online interactions. Consistent, integrated training in cybersecurity is essential—as Dr Prior aptly described, discussing online safety should be as routine as conversations about stranger danger.

Moreover, the practical strategies for mitigating risks include the use of unique and strong passwords, regular system updates, and the employment of password managers. These tools take on significant importance, especially in environments like schools where multiple accounts are common. Dr Prior advocates for maintaining an open dialogue about online security, helping young users understand the importance of vigilance and critical thinking when interacting with digital platforms.

As the dialogue surrounding substantial cybersecurity incidents continues to unfold, the necessity for comprehensive training and awareness programmes becomes increasingly apparent. Recognising that vulnerability is not confined to a specific demographic can pave the way for stronger protective measures, ultimately ensuring a safer online environment for all users in educational institutions.

### Reference Map

* Paragraph 1: (1), (3)
* Paragraph 2: (1)
* Paragraph 3: (4), (5)
* Paragraph 4: (1), (5)
* Paragraph 5: (1), (2), (4)
* Paragraph 6: (1), (3)
* Paragraph 7: (1), (4)
* Paragraph 8: (1), (6)
* Paragraph 9: (7)

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

## Bibliography

* <https://www.heraldscotland.com/news/25162681.schools-becoming-targets-cyber-criminals/?ref=rss> - Please view link - unable to able to access data
* <https://www.bbc.com/news/uk-scotland-edinburgh-east-fife-33425853> - In 2015, a malicious cyber attack on the City of Edinburgh Council resulted in the theft of over 13,000 email addresses from their 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. A council spokeswoman emphasized the importance of ongoing website security and collaboration with service providers to address associated risks.
* <https://news.stv.tv/east-central/phishing-attack-sees-edinburgh-pupils-locked-out-of-online-learning-materials> - In 2023, Edinburgh schools experienced a phishing attack that led to 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. As a precaution, the council reset passwords for all users, causing temporary access issues for staff and students. Secondary schools opened on a Saturday to assist students, especially those preparing for exams, in resetting their passwords. The council confirmed that no data was compromised during the attack.
* <https://www.huntress.com/industries/education/how-does-phishing-affect-schools> - Phishing attacks pose significant threats to educational institutions, with a notable increase in incidents targeting K-12 districts. In 2022, phishing scams affected 45 districts, doubling to 108 in 2023. These attacks compromise data security, disrupt operations, lead to financial losses, and result in legal and compliance issues. The loss of trust among students, parents, and staff is also a critical consequence. To mitigate these risks, schools are advised to educate staff and students on recognizing phishing attempts, implement password managers, change passwords regularly, use spam filters, update systems, and establish threat detection and response protocols.
* <https://cybertzar.com/phishing-attacks-in-schools-how-cybercriminals-target-staff-students> - Cybercriminals increasingly target schools through phishing attacks, exploiting the vast amounts of sensitive data schools manage and often weaker cybersecurity measures. In 2023, over 80% of UK schools reported cyber incidents, with phishing being a primary attack vector. Common tactics include fake IT support emails, business email compromise targeting headteachers and finance staff, parent payment scams, and ransomware deployment via phishing emails. The consequences of such attacks are severe, including loss of sensitive data, financial fraud, disruption of learning, and reputational damage. Schools are encouraged to implement multi-factor authentication, train staff and students to recognize phishing emails, block and monitor suspicious email activity, keep systems updated, and have an incident response plan in place.
* <https://www.ed.gov/teaching-and-administration/safe-learning-environments/school-safety-and-security/k-12-cybersecurity> - The U.S. Department of Education highlights the increasing frequency of cyber incidents in K-12 schools, with districts experiencing an average of five cyber incidents per week. These incidents range from data breaches to ransomware attacks and online class intrusions. Phishing emails and outdated software are identified as critical vulnerabilities exploited by cyber threat actors. The department emphasizes the need for schools to integrate cybersecurity into their emergency operations planning, providing training tools, best practices, and resources to support K-12 cybersecurity risk mitigation. Immediate strategies include keeping software up to date, implementing multi-factor authentication, using strong passwords, and educating staff and students to recognize and report phishing threats.
* <https://www.sterlingideas.com/phishing-cyberattacks-schools/> - Phishing attacks are a significant threat to educational institutions, with cybercriminals employing tactics such as scam phone calls, text messages, fake surveys, and educational content to deceive staff and students into revealing sensitive information or installing malware. These attacks can lead to compromised email accounts, unauthorized access to personal data, and disruptions in educational operations. The impact includes loss of sensitive data, financial fraud, disruption of learning, and reputational damage. To prevent phishing, schools should implement multi-factor authentication, use email filtering tools, encourage strong, unique passwords, keep software updated, educate the community on identifying phishing red flags, establish clear reporting protocols, and provide regular cybersecurity awareness training.