KEEPER®

Cybersecurity in Schools

Safeguarding Students in the Digital Era

Overview

As schools increasingly adopt digital tools such as learning platforms, virtual classrooms and connected devices, technology is becoming central to modern education. However, the rapid digital transformation of the 21st century also introduces new cybersecurity risks which educators cannot afford to ignore.

This 2024 Keeper Security report, derived from a study conducted of 6,000 individuals across Australia, New Zealand, Singapore, Indonesia, Japan, France, the UK, US and DACH regions, highlights a critical gap between trust and reality in the ability of schools to safeguard students in the digital era.

While many parents believe that schools are safeguarding sensitive information, persistent issues such as weak or reused passwords and limited cybersecurity education expose students to persistent threats including data breaches, identity theft and fraud. The findings emphasise the pressing need for schools and families to collaborate on stronger digital security measures and raise student awareness of online risks.

KEEPER

Current Cybersecurity Practices in Schools

Keeper Security's survey highlights a mixed landscape in school cybersecurity practices. While 74% of parents express confidence in their child's school to safeguard sensitive information, this confidence does not align with school practices. Only 21% of parents report that their schools provide guidance on creating and managing secure passwords, contributing to dangerous password habits. This is exemplified by 19% of respondents admitting to reusing passwords across personal and school accounts – heightening the risk of a widespread breach.

Confidence in School Cybersecurity Measures

18% Very confident

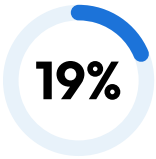
56% Somewhat confident

22% Not very confident

4% Not confident at all

Password Management Practices

Of schools provide guidance on secure passwords



Of respondents reuse passwords across accounts

Of schools provide access to a password manager

The limited availability of digital password managers, of which only 9% of schools provide access to, further exacerbates these risks. Password managers, which are essential for securely generating and storing complex passwords, and recommended by government agencies and cybersecurity experts, are notably absent, posing a clear opportunity where schools could significantly improve their cybersecurity practices.

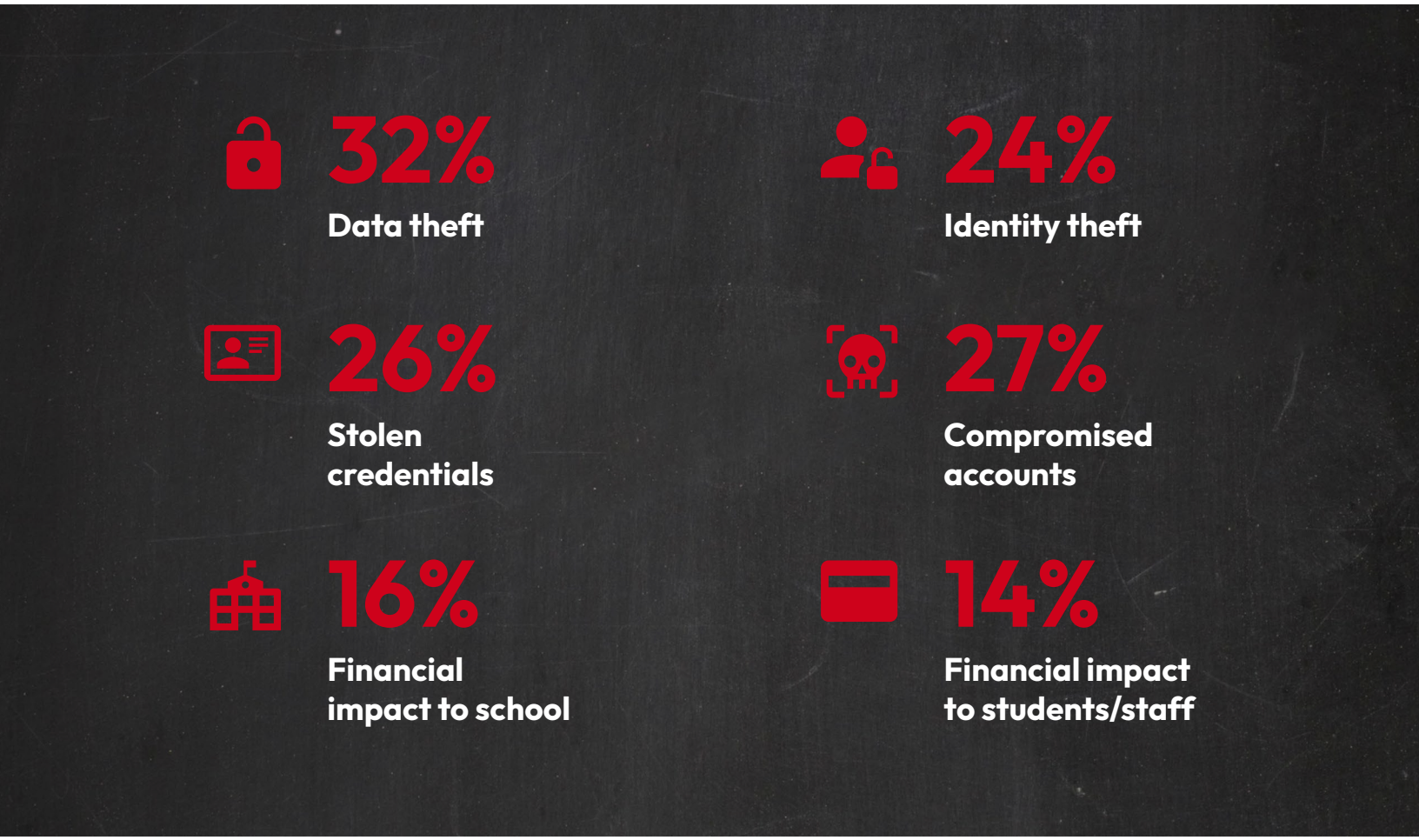
The Need for Enhanced Cybersecurity Education

Cybersecurity education within schools is dangerously sparse with only 14% of schools mandating security awareness training, and an additional 13% offering it optionally. This limited scope of mandatory training means many students are not receiving the latest education about online safety, leaving them vulnerable to evolving cyber threats. Effective cybersecurity training should not only focus on how to identify phishing scams, measures to protect devices and understanding the importance of regular software updates, but also on safely managing students' digital footprints.

Teaching students about the implications of their online activities, such as social media posts and browsing habits, is key to helping them protect their personal information. For example, cybersecurity education should emphasise the importance of adjusting privacy settings on social media platforms to limit public exposure. Educating students on how malicious actors can exploit their digital footprints to carry out future identity theft or targeted attacks is crucial for fostering responsible online behaviour.

Impact of Cybersecurity Incidents on Schools

Cyber attacks on educational institutions can have severe and far-reaching repercussions for students, teachers and administrators alike, underscoring the need for robust security measures to protect accounts and sensitive data. According to the survey, while only 7% of respondents report that their child's or their own educational institution has been hacked, the ramifications have been significant. When asked about the effects of such breaches, respondents indicated the following impacts:



The prominence of data and identity theft highlights the serious implications for both personal privacy and institutional security. The prevalence of stolen credentials and compromised accounts illustrates the extensive damage that such breaches can inflict, often resulting in exposure of sensitive information. Although the financial impacts are reported less frequently, they remain significant for both schools and individuals, showcasing that cyber attacks can inflict damage extending beyond immediate data and identity concerns.

The Role of Families in Cybersecurity

Parents and guardians play a vital role in reinforcing cybersecurity practices at home; however, Keeper's survey finds that 19% of families reuse passwords – a dangerous practice that can lead to multiple accounts being compromised through credential stuffing attacks. While many schools fall short in providing cybersecurity resources, families can help bridge the gap by using strong, unique passwords and Multi-Factor Authentication (MFA). MFA adds an additional layer of security to online accounts by requiring at least one extra form of verification to log in.

More than half (51%) of respondents report being very or somewhat worried about school cybersecurity, highlighting that while cybersecurity practices may be falling short, parents are aware of the risks. To address these risks, families should be proactive in monitoring their children's online activities and adhering to cybersecurity best practices in the home. This includes learning how to recognise suspicious emails and links, using strong and unique passwords, enabling MFA on all accounts that make it available and regularly updating software to protect against known vulnerabilities.

Moving Forward: A Unified Approach to Cybersecurity

Raising the bar for cybersecurity in our schools requires a collective and collaborative effort from both educational institutions and families of the students who attend them. Schools must enhance their cybersecurity education programmes, incorporate proven tools like password managers and expand training initiatives to cover cybersecurity best practices. Families should support these efforts by reinforcing good cybersecurity habits at home and actively participating in their children's digital education.

By working together, schools and families can create a safer online environment for students, maximising the benefits of technological advancements while minimising associated cyber risks.

Methodology

This online survey of 6,000 respondents in Australia, New Zealand, Singapore, Indonesia, Japan, France, the UK, US, and DACH – split evenly between students aged 16+, parents and the general population – was conducted by market research company OnePoll, in accordance with the Market Research Society's code of conduct. This survey was overseen and edited by the OnePoll research team. OnePoll are MRS Company Partners, corporate membership of ESOMAR, and Members of the British Polling Council.