Secure Mobility for Remote Education

Lookout helps schools K-12 provide a safe and engaging learning environment

When education can only be provided remotely

Schools traditionally rely on students and teachers to come together in classrooms to foster a safe and collaborative learning environment. However, when the need arises to move curriculums entirely online to enable remote learning, a new strategy is required. The priority becomes how to extend their influence into the household to preserve a positive learning environment where students feel safe and confident. Online access brings many benefits but also introduces risk to our impressionable youth if not properly controlled. Parents need the right coaching and technological controls to safeguard their children's privacy while also combating online threats such as offensive web content and cyberbullying.

Protecting students on their mobile devices

Students are connecting to learning platforms and video collaboration tools from their Chromebooks, mobile phones, and tablets to attend class. All of this occurs outside of the school's traditional security perimeter and introduces greater exposure to threats such as phishing, malware, and malicious web content. By blocking mobile phishing attacks, Lookout protects students from clicking malicious links embedded in email, SMS, apps, and social messaging. This type of attack is not only used by cybercriminals but also cyberbullies. Lookout also provides anti-malware to protect apps from malicious code and exploitable vulnerabilities. With Lookout, school administrators can set policies to block offensive web content so that students remain protected while browsing the internet. Collectively, these Lookout protections enable school administrators to deliver a safe online learning environment where students and families remain confident and embrace remote learning.

Challenges

1. Children are often left unattended while online and need protection against offensive web content.

2. Cyberbullying is a real threat that can have negative emotional consequences for a student.

3. Schools must protect student privacy amidst increasing mobile threats such as phishing attacks.

Lookout Critical Capability

Lookout filters offensive content on Chromebooks, Android, and iOS devices by inspecting all outbound connections made by the device and apps at the network level at the time a user attempts to connect. This approach does not rely on inspecting message content, and therefore respects user privacy. Lookout also provides 360-degree phishing protection across email, SMS, messaging apps, and apps containing URLs that download malicious plug-ins. By identifying offensive content, Lookout enables system administrators to extend their influence into the household to protect students from cybercriminals and cyberbullies.

MOBILE RISK MATRIX

Lookout has developed the following matrix to help you understand the mobile risks that are most relevant to your school. These risks fall into four main categories; mobile phishing, web content, malware, and network threats. With Lookout, you can protect your teachers, students, and their families from these mobile threats.

Lookout Protection for Schools K-12

THREAT	PROTECTION	LOOKOUT
Mobile Phishing	• Malicious links in email, SMS, and social messaging are blocked • Cyber criminals and cyberbullies use phishing	✔
Malicious Web Content	• Prevents access to malicious web content • Set policies to allow and block specific websites	✔
Malware	• Detect apps that leak data or breach school security policy • Detect apps that breach regulatory compliance	✔
Network Threats	• Block access to rogue Wi-Fi networks • Detect man-in-the-middle attacks	✔

Why Lookout

Lookout Mobile Endpoint Security with Continuous Conditional Access ensures security and compliance on every device, leveraging a large data set fed by nearly 200 million devices and the analysis of over 100 million mobile apps. With the Lookout Security Platform, it's easy to deploy Lookout and apply security policies across the entire school organization. Students and teachers receive alerts and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by dynamic device health checks to provide Continuous Conditional Access to sensitive applications and data.