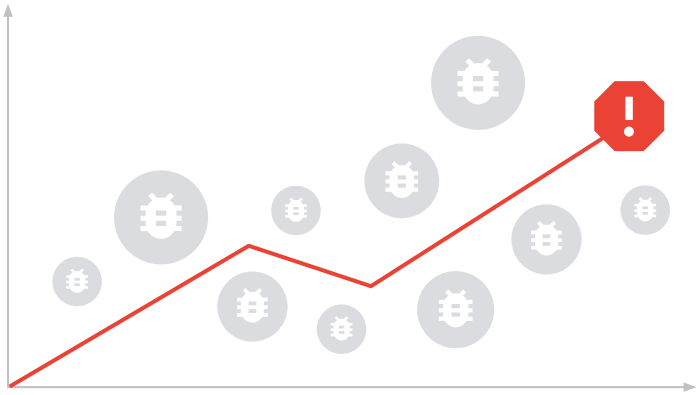
Google for Education

Keep your institution safer online

In today's rapidly evolving cyberthreat landscape, educational institutions are top targets. In fact, **80% of school IT professionals** reported that their schools were hit by ransomware attacks in 2022.*



Be ready for tomorrow's threats

Learn **best practices** to reduce the risk of successful cyberattacks and enable safer learning.

01

Safeguard data with secure authentication

Verify users are who they say they are with two-factor authentication, single sign-on, passwordless authentication, and more.

02

Apply the right security settings

Configure settings so users can't change them, limit how many apps they can install, and lock lost or stolen devices.

03

Update and upgrade your systems

Install the most recent versions of your OS and browser, and enable automatic updates.

04

Use real-time alerting and monitoring

Identify what you need to protect, collect the right data, and ensure security tools are always logging events across your systems.

05

Teach digital safety

Educate your school community on common threats and safe data sharing. Share internet safety resources like Be Internet Awesome.

*Sophos, The State of Ransomware in 2023, July 2023

Learn more about privacy and security at edu.google.com/privacy-security

Google never stops protecting your digital safety

Enable a safer way to learn online with the privacy and security capabilities that Google uses in our own tools to protect billions of people every day.

Every day
100 million
phishing attempts are blocked by Gmail.

Every week
300,000
unsafe websites are identified by Google.

Every day
74 million
people get help from Google's Password Manager.

Every year
700 million
people strengthen their security with Security Checkup.

Google for Education, K-12 Cybersecurity Guidebook

Secure by default. Private by design. You're in control.

Our EdTech provides you with built-in security that's compliant with the highest global standards, full control of your data and security policies, and simple, ad-free tools that help students fully immerse themselves in learning.

chromebook

Chromebooks run on ChromeOS, the leader in cloud-based computing.

Zero reported successful ransomware attacks on Chromebooks.

Verified Boot is a Chromebook's way to self-check and repair itself upon startup.

Automatic updates keep Chromebooks prepared for evolving threats.

Security sandbox confines webpages and apps, if you land on malicious ones.

Automatic data encryption ensures a user's space can't be accessed by others.

Google Workspace for Education

Google Workspace is one of the most secure cloud-based communication and collaboration suites.

Zero actively exploited software vulnerabilities in Google Workspace since November 2021.*

Alert center gives you a complete view into your security with alerts and actions you can take to address threats.

Automated data loss prevention tools let you set your own rules in Drive and Gmail to prevent data loss or theft.

Secure authentication tools like two-factor authentication and single sign-on help protect sensitive data.

Data retention policies set with Vault allow you to control how data is stored and for how long.

* Google for Education, K-12 Cybersecurity Guidebook

Learn more about privacy and security at edu.google.com/privacy-security