The stakes for effective cybersecurity are higher than ever

Find out more below about Google's work to make a safer internet

Safer with Google

Governments and businesses are at a watershed moment in addressing cybersecurity.

Safer with Google

Cyber attacks are increasingly endangering valuable data and critical infrastructure, and governments and companies are facing key challenges:

Organizations continue to depend on **vulnerable legacy infrastructure**, which is more vulnerable to compromise than modern IT supported by security best practices. Too much reliance on legacy vendor contracts can limit competition and choice, inflate costs, and create privacy and security risks.

Nation-state actors, cybercriminals and other malicious actors continue to target vulnerabilities, whether through ransomware, software supply chain compromises, phishing, or other practices. **Many organizations lack the tools or expertise to stop them.**

Governments and businesses often **don't have the resources and trained professionals** to anticipate and deal with these threats on their own.

We keep more people safe online than anyone else.

Learn more about how we are collaborating to make the internet a safer place

1

Products

Every single product we make is secure by default

2

Ecosystem

We're driving the industry to create a safer internet

3

Businesses

Our industry-leading security and enterprise offerings protect organizations and businesses of all sizes

4

Governments

We protect governments and high-risk users by countering threats and modernizing infrastructure.

Every single product we make is secure by default.

Protecting people wherever they browse

Today over 4 billion devices are automatically protected by our **Safe Browsing** technology. And to provide even greater protection, last year we launched Enhanced Safe Browsing in Chrome, which has already reduced phishing by 35% for users who opted in.

Helping people sign in safely

Believe it or not, today's most common online security risk is bad passwords. Google's **Password Manager** helps create, save and manage passwords for any account. And **every day, Google checks 1 billion saved passwords** and provides automatic alerts if we detect any have been compromised in a data breach.

Email that keeps people's private information safe

Many malware and phishing attacks start with email. To keep you safe, **Gmail blocks more than 99.9% spam, phishing attempts and malware before they ever reach your inbox**. Across all of our users, this equates to more than 15 billion blocked messages every day.

Keeping devices safe from bad apps

Every day, **Google Play Protect** runs security **scans on 100 billion installed apps** around the world. If we discover a malicious app, we quickly alert the user and instruct them on how to remove the app from their device.

Encrypting data to provide the highest level of security and privacy

When you send an email on Gmail, share a video on YouTube, ask a question in Search, or store your photos in Google Photos, the data you create moves between your device, Google services and our data centers. We protect this data in transit and at rest with multiple layers of security, including leading encryption technology like **HTTPS** and **Transport Layer Security**.

Computers that protect your sensitive data—at school, work and home

Chrome OS is a cloud-first platform that powers Chromebooks and provides protection against ransomware by default. In fact, **there have been no reported ransomware attacks ever on any business, education, or consumer Chrome OS device**.

100B

installed apps scanned for malware every day

15B

spam messages blocked every day

4B

devices protected from malicious sites every day

Making important security technology available to others, to raise the bar for security everywhere.

We collaborate to drive toward a more secure internet ecosystem

Opening sourcing our security technology for companies and developers around the world

We've led the way on developing open source technologies that help make the whole internet safer. For example, we made **Safe Browsing** technology free so that other browsers and developers can check URLs against our lists of unsafe websites. **We also founded and continue to lead the Data Transfer Project (DTP), with Microsoft, Twitter, Facebook, and Apple, that enables people to securely move their data between service providers.**

Securing software supply chains for a stronger infrastructure

We worked with the Open Source Security Foundation (OpenSSF) to develop and release Supply Chain Levels for Software Artifacts (SLSA or "salsa"), a proven framework for securing the software supply chain. In our view, wide support for and adoption of the SLSA framework will raise the security bar for the entire software ecosystem. **We also pledged to provide $100 million to support third-party foundations, like OpenSSF, that manage open source security priorities and help fix vulnerabilities.**

Enabling adoption of secure Cloud products through engineered-in security

We've successfully built advanced, cloud-native defenses from the ground up to serve individuals, governments and businesses around the world at massive scale. As organizations move to the cloud, they can transform their security posture with innovations such as embedded data loss prevention, confidential computing, and built-in risk management.

Making multi factor authentication easy and widespread

We led the invention of security keys and were the first to build a security key right into the phone, so that **today over 2 billion devices automatically support the strongest, most convenient 2-factor authentication technology available.** Leveraging this technology, we continue to move away from the memorized passwords of the past and lead the way toward a more secure, password-free future.

$10B

Invested over the next five years to strengthen cybersecurity, including expanding zero-trust programs, helping secure the software supply chain, and enhancing open-source security.

$100M

pledged to provide to support third-party foundations, like OpenSSF

Establishing new standards and driving broad adoption.

Helping secure sites across the web through encryption

Backing our services with HTTPS encryption ensures you can securely connect to sites and enter your private information like credit card numbers without anyone intercepting your information. We've helped the rest of the web make this important move to HTTPS by providing tools and resources to all developers. Today, **HTTPS secures 90% of all websites.**

We've published over 160 academic research papers

on computer security, privacy, and abuse prevention, and we warn other software companies of weaknesses in their systems. Beyond securing our own products, **interested Googlers also spend some of their time on research that makes the Internet safer, leading to the important discovery of bugs like Heartbleed.**

Enabling others to gain valuable skills

Since launching Grow with Google in 2017, we've helped over 7 million Americans get training in digital skills. We are now pledging, through the Google Career Certificate program, to train 100,000 Americans in fields like IT Support and Data Analytics, learning in-demand skills including data privacy and security.

Building a safer, more trusted internet

Today, Google teams work across privacy, security, content responsibility and family safety to make every day safer with Google. Led by experienced teams of engineers, policy specialists and subject matter experts, we take a holistic approach to understand the problem, develop solutions and partner with others to empower people everywhere. Together we are leading the way toward a better, safer Internet for all.

90%

of all websites are secured by HTTPS

10M

Americans will be trained in digital skills from basic to advanced by 2023

We've built one of the world's most secure and reliable cloud infrastructures.

Leading the way with zero trust

Over a decade ago, Google pioneered an approach we all now know as "Zero Trust," in which no person, device or network enjoys inherent trust. While many are now out there selling zero trust products, Google has embedded Zero Trust as a core element of our design philosophy. Whether it's how developers build new software; how applications talk to each other, or how employees; contractors and remote workers access systems; Zero Trust capabilities mean that there are fewer attack vectors, fewer opportunities to lose data, and more control over the systems businesses depend on.

Modernizing Security Operations

The scope and scale of securely operating in the cloud can be daunting to organizations. Google has taken what it has learned and built Chronicle, our approach to Security Operations at cloud scale and speed. Organizations can detect every security activity in their environment , map it to threat intelligence, and quickly respond, all without needing to massively grow their operations center.

Protecting data 24/7 with our cloud infrastructure

From custom-designed data centers to private undersea cables that transfer data between continents, we operate one of the world's most secure and reliable cloud infrastructures. It's continuously monitored to protect your data. And in the event of a disruption, platform services can be automatically and instantly shifted from one facility to another so that they can continue without interruption.

Moving from Shared Responsibility to Shared Fate

Google is pioneering the shared-fate model for risk management in conjunction with our customers. We believe that it's our responsibility to be active partners as our customers deploy securely on our platform, not delineators of where our responsibility ends. We stand with you from day one, helping you implement best practices, manage risk, and even financially protect your cloud investment.

24/7/365

We develop and deploy infrastructure software using **rigorous security practices**. Our operations teams detect ⚠ and respond to threats to the infrastructure from both insiders and external actors, 24/7/365.

Protecting enterprises from common web-based attacks.

Protecting websites from fraudulent activity, spam, and abuse

With reCAPTCHA Enterprise, websites are protected against common web-based attacks like credential stuffing, account takeovers, and scraping and help prevent costly exploits from bad actors and automated attacks.

Preventing employee phishing and account takeovers

Compromised credentials are one of the most common causes of security breaches. While strong authentication solutions exist, a determined attacker can circumvent them. We worked to create and implement new modern authentication standards along with hardware Security Keys that use public key cryptography to verify users' identity and the URL of the login page, making logins essentially unphishable.

Eliminating endpoint compromises and ransomware

Today, **Chrome protects more than 2 billion active users** with advanced technology like site isolation, sandboxing, warnings for dangerous sites and downloads, and automatic security updates. We extended this idea of secure by default endpoints to create Chrome OS - a purpose-built operating system for the Cloud that prioritized security above all else.

2B

active Chrome users protected with advanced technology

We combat the world's most sophisticated adversaries to protect governments and high-risk users.

Guiding industry-wide security transformation with the Google Cybersecurity Action Team

We recently formed the Google Cybersecurity Action Team, bringing together the world's premier security experts to advise organizations on deploying effective cyber defense solutions. From their first transformation roadmap and implementation, through increasing their cyber-resilience preparedness for potential events and incidents, and engineering new solutions as requirements change, GCAT guides organizations through the full cycle of security transformation.

Countering hacks with Google's Threat Analysis Group

Google's Threat Analysis Group (TAG) works to counter targeted and government-backed hacking against Google and our users. The group's work involves detecting and defeating threats, and warning targeted people and customers about the world's most sophisticated adversaries, protecting the full range of Google products including Gmail, Drive and YouTube.

Protecting at-risk groups with Project Shield

Project Shield uses our advanced security technology to protect news, human rights organizations, election sites, political organizations, and campaigns and candidates from distributed denial-of-service (DDoS) attacks. No matter the size of the website or the size of the attack, Project Shield is always free. Project Shield **has customers from over 100 countries, and is actively proxying traffic for sites in over 50 countries at any time.** We've protected public security resources, including krebsonsecurity.com, which have helped to identify threats and enable response by the security community and law enforcement.

Securing those at risk of targeted attacks with the Advanced Protection Program

The Advanced Protection Program is Google's strongest account security offering and the industry's first free program designed to safeguard the personal and enterprise Google Accounts of those at higher risk of targeted online attacks. 140 federal campaigns chose APP to protect themselves from targeted cyber attacks during the 2020 US election season. To date, we've seen zero evidence of a successful phishing attempt on accounts enrolled in the program.

Defending Digital Campaigns and the International Foundation for Electoral Systems

We work with bipartisan and democracy-promoting organizations around the world to help make all qualifying campaigns and elections safer, by educating campaign teams on advanced security protections like our Advanced Protection program.

140

140 federal campaigns chose APP to protect themselves from targeted cyber attacks during the 2020 US election season.

Learn more at safety.google