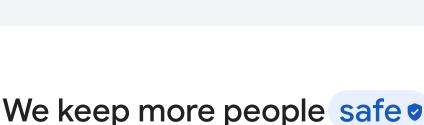




through the years

Our cybersecurity journey

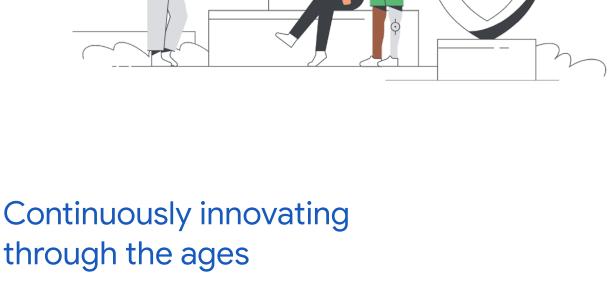


online than anyone else in the world

G Safer with Google

With the dramatic rise of state-sponsored cyber attacks and malicious actors online, we believe our products and services are only as helpful as they are secure.

At Google, we are more focused than ever on protecting people, organizations and governments by sharing our expertise, empowering the society to address ever-evolving cyber risks and continuously working to advance the state of the art in cybersecurity to build a safer world for everyone.



Developing secure products and platforms

Fostering programs Providing critical funding for and partnerships innovation and workforce training As people's needs and the internet evolve, we continue to be at the forefront of new technologies to mitigate ever-changing cyberthreats,

- 2004

2007 **Gmail Spam Protection** Safe Browsing We were the first to build Al-driven We help proactively protect devices around security protections into email. the world by alerting users when they visit

99.9% of dangerous and suspicious emails are blocked **A** by Gmail

2009

We acquired the fraud and bot management

account takeovers, and to prevent abusive

activities from malicious software/fake users.

solution to stop credential stuffing and

▲ 5 Million websites defended ●

reCAPTCHA

2010

Zero Trust After surviving Operation Aurora, a

coordinated series of cyber attacks, we

revolutionized our approach to build a

as "Zero Trust". It ensures fewer attack

vectors, fewer opportunities to lose data,

secure-by-default architecture now known

2008

in 2020.

5 Billion devices

protected • by Safe Browsing

across platforms. 1 Billion passwords checked • daily for breaches

now used for 50% of all logins in Chrome

Google Password Manager

The introduction of Password Manager made

signing-in easier and safer, without the need

to remember or type in your password and is

dangerous websites, evolving these online

protections into Enhanced Safe browsing

2010 **Threat Analysis Group** (TAG)

detecting, analyzing, and disrupting government-backed and serious criminal cyber threats. TAG traced Wanna Cry, the largest ransomware attack in history, to North Korea, and recently shared examples of the hack-for-hire ecosystems from India, Russia,

and the United Arab Emirates.

specialized team of experts responsible for

After Operation Aurora, we formed a

and more control over the systems users depend on. We support the White House's efforts to deploy the Zero Trust model across the federal government and have also

packaged it into BeyondCorp Enterprise so that any enterprise can leverage it.

2010 Google Bug Hunters Our Vulnerability Rewards program attracts

high schoolers, lawyers, IT professionals, and

products with cash prizes. Their motives vary,

Project Shield has helped protect news, human

undiscovered vulnerabilities to keep online

hobbyists to hunt down bugs in Google

but their mission is the same: find

Launched to take on an adversarial mindset and hack Google to help strengthen our defenses and spot gaps. They work across the globe to keep up with current threats,

better frameworks.

The Red Team

2010

improve security controls, conduct attack detection/prevention, and eliminate entire classes of vulnerabilities by driving new and

2011 2-Step Verification

We were one of the first to offer 2-Step

in. Even if your password is stolen, your

50% decrease in compromised

Verification (2SV) by default, and the first to

auto-enable 2SV for over 150 million people

in 2021, providing a safe and easy way to log

Millions of dollars paid out in rewards since 2010

services safe and secure.

2013

rights organizations, election sites, political organizations, and campaigns from Distributed Denial of Service (DDoS) attacks in over 100 countries from cyber attacks by identifying threats and enabling responses in the security community and law enforcement. 150+ websites currently

protected o in Ukraine

Project Shield

2014 **Project Zero** A specialized task force devoted to hunting zero day exploits across the internet - in

software, hardware, Google products, and beyond to ensure a safe and open Internet. They were the first to detail "Meltdown" and "Specter," enabling developers to quickly address CPU vulnerabilities and apply

mitigations across the software supply chain.

2017

Advanced Protection

Program (APP)

account is protected.

accounts since 2SV

Extra secure protections, including Security Key, for high-visibility and high-risk users such as journalists and government officials. 300+ federal campaigns protected •

Google Play Protect

The most widely deployed mobile threat

adapting and improving with Google's machine learning, Google Play Protect

Q 100+ Billion apps scanned for malware daily

150 Million user

payments encrypted daily

protection service in the world, constantly

automatically scans apps for malware and

encrypts user payments on Android phones.

Passwordless Re-Authentication Extended our FIDO support in Android so users could seamlessly log on to websites with just a

2019

2018

Titan Security Key

too, not just with Google.

We made the Titan Security Key for users who

want an end-to-end Google solution. The keys are FIDO compliant and can be used elsewhere

PIN or biometric, no password needed.

2019

Chronicle

2021

the cloud.

2022

Post-Quantum

Cryptography

Standardization

Future focused, we continue to develop

cryptosystems and compromising digital

communications. The National Institute of

Standards and Technology selected a

submission with Google's involvement

(SPHINCS+) for standardization.

next-generation cryptographic systems that

safeguard against the breaking of public-key

network data.

Built as a specialized layer on top of our core

infrastructure, Chronicle was introduced to

provide cloud-based security designed for

enterprises to privately retain, analyze, and

search massive amounts of security and

Confidential Computing

For critical security, safety, and privacy, we

Computing, a breakthrough technology that

while at rest or in transit. Now even the most

sensitive data can confidently be migrated to

introduced Google Cloud Confidential

keeps data encrypted while it is being

throughout its entire life cycle, including

processed, allowing it to stay secure

2021 Investment to Advance Cybersecurity We're committed to strengthening

2017

cybersecurity initiatives

Google Open Source

Security Team (GOSST)

of the open source software the world

relies on. We partnered with the Open

Source Security Foundation (OpenSSF) to

develop and release Supply-Chain Levels

to secure the software supply chain and

enable long-term security for the entire

\$100 Million committed to third party

software ecosystem.

for Software Artifacts (SLSA), a framework

GOSST was created to improve the security

\$10 Billion commitment to

Certificate program.

2021

cybersecurity, expanding zero-trust

programs, helping secure the software

Analytics through the Google Career

supply chain, and enhancing open-source security. We pledged to train 100,000

Americans in fields like IT Support and Data

open source security operations to help fix vulnerabilities 2022 **Protected Computing**

We announced Protected Computing, a

transforms how, when, and where data is

privacy and safety. We do this by minimizing

the data footprint, de-identifying data, and

means Android can suggest the next phrase

in the text, while keeping the conversation

restricting access to sensitive data. This

completely private.

processed to technically ensure user's

growing toolkit of technologies that

cloud-native security offerings, we help enterprises and public sector agencies stay protected throughout the security lifecycle.

Mandiant brings real-time, in-depth threat

Passwordless Future

Sign-in standards to Android & Chrome

finally have the platform for a truly

passwordless future.

through passkey technology in 2023, we will

We've been setting the stage for a passwordless future for over a decade. We joined the FIDO Alliance in 2013 to drive open standards for a passwordless world and now by expanding our support for FIDO

Passkey: The

2023

In an age of ever-expanding technological reach, trust in technology

intelligence gained on the frontlines of cybersecurity with the largest organizations in the world. Combined with Google Cloud's

2022

Mandiant and

Google Cloud

is key to unlocking society's true potential. As we put our security knowledge into practice, we will continue to partner with people, businesses, and governments to protect their safety and drive a new era in cybersecurity.

Protecting people, businesses and governments

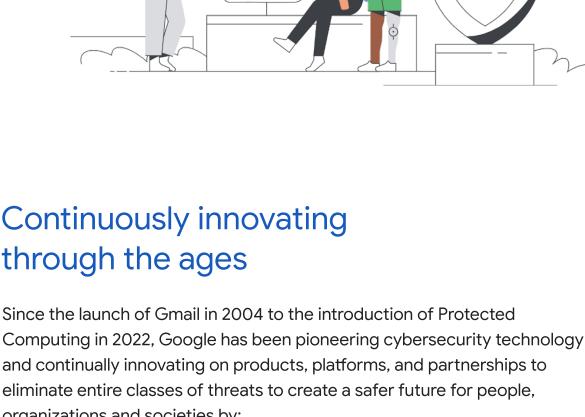


Advancing future technologies We want to protect societies from the next generation of

cyberthreats. Building on our AI expertise, we are designing the next wave of architectures to push the boundaries of security innovation.

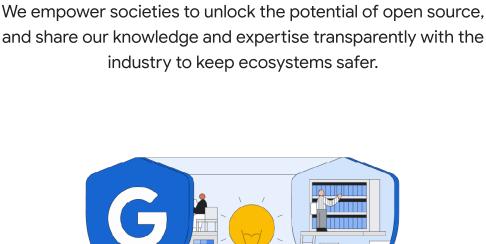


Every day you're safer



organizations and societies by: Building agile Security Teams ensuring that every day is safer with Google.

Security is the cornerstone of our product strategy. Which is why all our products have built-in protections that make them secure by default.



with Google

Visit g.co/safety/cyber ☑

Google