Talk Nerdy To Me

July 2022

How Old Is Google? History Of The World’s Most Popular Search Engine

According to tech company EarthWeb, Google processes about 8.5 billion searches per day. With Statista’s estimate of 1.88 billion total websites on the Internet as of August 2021, the scope of Google is still far from reaching the massive number after which it was named — but it grows larger by the day. Originally conceptualized as a search engine, the company has grown immensely since its founding. Google also owns YouTube, and its purchase of Android allowed the company to establish itself in the phone market with products like the Google Pixel smartphone.

How old is Google?

Google Inc. was founded by Larry Page and Sergey Brin on Sept. 4, 1998, following a $100,000 investment from Andy Bechtolsheim, co-founder of Sun Microsystems. According to History, Page and Brin filed for Google’s initial public stock offering on April 29, 2004. The company went public in August 2004.

Google acquired Android in 2005 for $50 million, an investment that is paying off. Statista data reveals that over 80% of smartphones across the globe have run Android operating systems since the year 2014.

In early October 2006, Google purchased YouTube for $1.65 billion. As of June 2022, Susan Wojcicki, Google’s 16th-ever employee, is the CEO of YouTube.

Google renamed its company Alphabet in 2015, making Google a subsidiary. This move was intended to avoid antitrust violations and unite all the company’s acquisitions and services as a technology conglomerate.

In 2019, Page and Brin stepped down from their respective roles as CEO and President. The company’s current CEO is Sundar Pichai.

Source: usatoday.com

Make Sure You’re Not Ignoring The Biggest Cybersecurity Threats

Securing your network against cyber threats can be challenging -- but taking care of the basics can go a long way towards keeping hackers out.

Cybersecurity is hard. Technology is continually changing, cyber criminals’ tools and techniques are always evolving and maintaining the security of a network with users who each want to do their own thing without being restricted by security is a constant challenge.

Ransomware remains a significant problem, as cyber criminals threaten to encrypt networks and victims give into their extortion demands for the decryption key, while cybersecurity agencies in the US and the UK have issued warnings about the potential rise in cyber threats as a result of Russia’s invasion of Ukraine.

Remote work is making easy targets for hackers
For many businesses, hybrid and remote working has become the norm in recent years and organizations have shifted towards cloud-based applications and services to enable this.

But while this shift has been effective for productivity and improving employee happiness, hybrid working also comes with additional cybersecurity risks that organizations might not be thinking about -- and that’s making life easier for cyber criminals.

For example, cloud applications like Microsoft Office 365 and Google Workspace offer employees the ability to work from anywhere -- but if a malicious hacker got hold of their username and password, they could enter the network. That’s especially true if the password is weak enough to be cracked in a brute force attack.

It’s also possible that entire sections of the network containing sensitive information could be exposed to the open internet due to cloud misconfigurations. In these instances, attackers might not even need a password -- they can just walk right in and raid the server for exposed information.

Simple cybersecurity updates are being ignored
But it isn’t just security vulnerabilities in cloud-based applications that are flying under the radar or outright being ignored. For one reason or another, cybersecurity teams often struggle to manage vulnerability management and patching across the board.

Applying security patches as quickly as possible is often said to be one of the best things to help protect networks from cyberattacks -- but new vulnerabilities regularly appear, and many information security teams aren’t keeping up.

Add to this the unknown security flaws that can lurk within software that many companies use every day and assume is secure. For example, Log4j was a significant vulnerability that emerged in December last year and one which Jen Easterly, director of US cybersecurity and infrastructure agency CISA, described as “one of the most serious that I’ve seen in my entire career, if not the most serious”.

Cyber criminals began trying to exploit it almost immediately and businesses were told to apply the patch as quickly as possible. But months later, many still hadn’t applied the updates, leaving their organizations vulnerable to network intrusions.

Cybersecurity basics can go a long way
When it comes to securing cloud services, emails and the wider network, there are steps that information security teams can take that can help protect users -- and the network -- from most cyberattacks.

First, applying security patches as soon as possible prevents cyber criminals from exploiting known vulnerabilities in software to enter or move around networks, so it should be a pillar of cybersecurity strategy for any organization in any sector.

Rolling out multi-factor authentication (MFA) can also provide a significant barrier to cyberattacks, because it means that -- even if a hacker has a legitimate username and password -- they’re unable to take control of a cloud service or email account without the user approving it. According to Microsoft, using MFA blocks over 99.9% of attempts at hacking into accounts.

In addition to this, encouraging users to avoid using and re-using simple passwords makes accounts more difficult to break into. Using a password manager can help with this.

To many people, these measures might sound like basics of cybersecurity -- but in order to ensure that people and networks are safe from cyberattacks, the basics need to be put in place before anything else.

Source: https://www.zdnet.com/article/tech-security-the-next-challenges/

Our CEO Is A Published Author

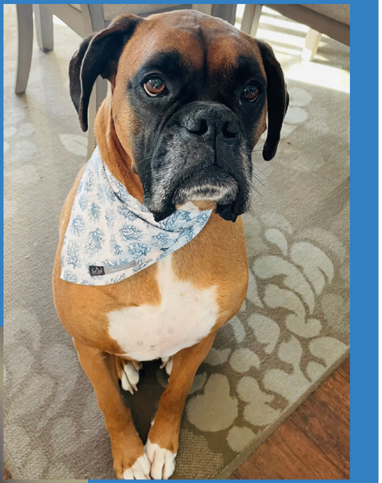
Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

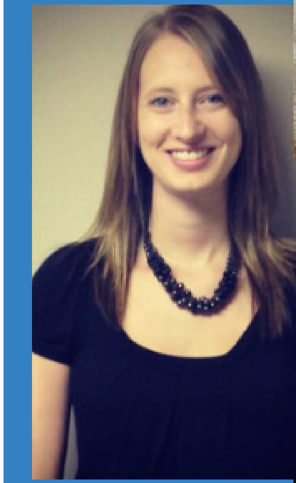
In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

July Birthdays!

Happy birthday to all of our PITG July birthdays!





Grabbing The Bull By The Hornes - Preferred IT CEO, Jason Horne, Is Gaining Ground Fast

Check out Preferred IT Group's CEO, Jason Horne in MSP Success Magazine!

"So, in the sports bar that night, where patrons sampled cold beer and cheered on the Cubs and Komets, a vision for what would become Preferred IT emerged."

MSP SUCCESS
MAGAZINE
Grabbing The Bull By The Hornes
Preferred IT CEO, Jason Horne, Is Gaining Ground FAST
Page 14
Marcus Lemonis Reveals
Now Is The Time To Double Down On Marketing
Page 22
LANDING YOUR MOON SHOT
Buzz Aldrin Talks About Hitting BIG Goals
Page 8
Determination That Won't Quit
Shark Tank's Barbara Corcoran's Rise To New York Realty Royalty: How You Can Dominate Sales Like The Queen
Page 17
MSP SUCCESS
Special Edition: Winter 2022
MSPSuccessMagazine.com
Jason Horne, Co-Founder Of Preferred IT Group

FUN FACT!

Wikipedia is maintained by thousands of bots!

preferred group IT

CONTACT US

Fort Wayne 260.440.7377	Warsaw 574.306.4288
Columbia City 260.213.4266	Indianapolis 317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.