

whoownsme.com

Who Owns Me is a website that lists other websites, applications and hardware that gathers your personal data or records analytics based on your usage and uploads it to their databases without your consent and therefore figuratively own a piece of you. Whoownsme.com categorises everything in a manner that makes it easy to navigate and even provides a search function to instantly find what you're looking for. Something like this can be very beneficial given the silent and undisclosed nature of these privacy breaches and can work towards informing those unaware of what their apps and devices are doing in the background.

My website will follow google's own material design rules to resemble the misleadingly safe and accessible aesthetic of the apps that breach your privacy.

It will allow you to narrow down your search based on what device you own and what types of apps your using, it will then let you sort and/or filter the results by different queries.

The idea came from project 1 of Design as Inquiry where I chose an article on a "smart home" fitted entirely with devices that connect to one another and the internet to supposedly make life easier. This article described each devices interaction with outside servers and detailed what was being sent, when it was being sent and how much was being sent.

The format in which this project is presented is inspired by the website <https://twofactorauth.org/> which compiles a list of websites and apps that require an account registration and state whether they give the option to use an email or phone to log in along with your password in order to improve security. Also known as Two Factor Authentication (2FA). Twofactorauth specifies the different types of 2FA and if those apps/sites support them, they also leave handy links to contact developers of programs that don't have 2FA to request the feature.

Who Owns Me will tell the user the name of the app/device, the name of the developer/company behind the app/device, all security and privacy breaches along with extra notes on those breaches and each entry will be given a severity rating based on how malicious the breaches and practices are.

Who Owns Me's purpose is to inform and educate on the safety of specific programs so the user is able to take caution when it comes to dealing with them and make decisions based on the information we've compiled. While twofactorauth details a list of potential privacy threats, whoownsme is a list of definite privacy breaches and sketchy practices designed to benefit the companies involved.

This is an important role to fill as even I who considers myself quite tech savvy, have been pretty oblivious to privacy breaches like this due to their silent nature.

Who Owns Me?

A list of software and hardware that gather your information and breach your privacy



All



Apps/Websites



Hardware



All



Apps/Websites



Hardware



Apps



Websites



Windows



Android



iPhone



MacOS



Other Devices

Application	Company	Breaches	Notes	Malicious Rating
				Severe
				Mild

Logo

Who Owns Me?

Made with **Google's** own
deceptively innocent looking logo font

Google being guilty of using people's data
for the sake of targeted ads



All



Apps/Websites

Simple flat art style with
clear fonts and simple
colours

Follows Google's own
material guidelines

Fonts

Product Sans (Logo)

<https://befont.com/product-sans-font.html> {might not be official link}

Product Sans

a

Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm
Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz

*Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm
Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz*

1234567890+-=_[]{}|\'"/";,.,?!<>~@#\$\$%^&*()

Roboto (Website text)

<https://fonts.google.com/specimen/Roboto>

Roboto

SUNGLASSES

Self-driving robot lollipop truck

Fudgedicles only 25¢

ICE CREAM

Marshmallows & almonds

#9876543210

Music around the block

Summer heat rising up from the boardwalk

Both fonts are used within the material design guidelines and thus are perfect fits for my website's aesthetic

Similar Websites

<https://twofactorauth.org/>

As mentioned in the brief, twofactorauth details a list of apps and websites and states whether they support two factor authentication (2FA) or not.

Two Factor Auth (2FA)

List of websites and whether or not they support 2FA.

Add your own favorite site by submitting a pull request on the [GitHub repo](#).

Search websites

Backup and Sync Banking Betting Cloud Computing Communication

Communication	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
Action Network						✓
Basecamp	Tell them to support 2FA on Twitter via Email					
Campfire						

<https://haveibeenpwned.com/>

A site that lets you know if your own account had been compromised in a data breach

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address **pwned?**

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)


Why 1Password?

397 pwned websites 8,418,474,549 pwned accounts 99,584 pastes 121,023,090 paste accounts

Largest breaches Recently added breaches

<https://www.malwarebytes.com>

Malwarebytes has an interesting section on data/privacy/security related jargon

For HomeFor BusinessPricingPartnersResourcesSupportCompanySign inFREE DOWNLOAD

Data Breach

A data breach comes as a result of a cyberattack that allows cybercriminals to gain unauthorized access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of the customers or users contained within.

Cybersecurity Basics

JUMP TO

Data Breach

- Latest data breach news
- What is a data breach?
- How do data breaches happen?
- Is my stolen data encrypted?
- What do criminals do with my data?

What is a data breach?

The Malwarebytes Labs blog called 2018 [the year of the data breach](#). What a year it was. The list of companies that were hacked by cybercriminals reads like a who's who list of the world's biggest tech companies, retailers, and hospitality providers—and that's only the data breaches that we know about. In many instances, an organization or company won't even know they've been breached until years later. According to the Ponemon Institute's 2018 *Cost of a Data Breach* study, a data breach goes undiscovered for an average of 197 days. It takes another 69 days to remediate the data breach. By the time the security failure is discovered and fixed, the damage is already done. The criminals responsible will have enjoyed unfettered access to databases full of valuable data—your valuable data. Not to mention the data of hundreds of millions of people like you who had the bad luck of doing business with a company that got hacked.


Who doesn't like cookies?

We use cookies to help us enhance your online experience. If that sounds good, click "Accept All Cookies" or to review our Privacy and Cookie Policy click [here](#).

✓ Accept All Cookies

<https://ghostproject.fr>

Similar to haveibeenpwned

HomeFAQTOSPrivacyDonate

DATABASE LOOKUP OF

READY TO TRY

GhostProject?

The total amount of credentials (usernames/clear text password pairs) is "1,400,553,869 . . .";

Search by full email address or username. Example: user@test.com, usertest, *@test.com..

Search

This website uses cookies to ensure you get the best experience on our website. [Learn more](#)

Got it!

Potential Site Ad:

**You belong to
someone else.**

Find out who that someone is

whoownsme.com

You're giving
much more than
your money for
your devices

Who Owns Me?

Find out who at *whoownsme.com*