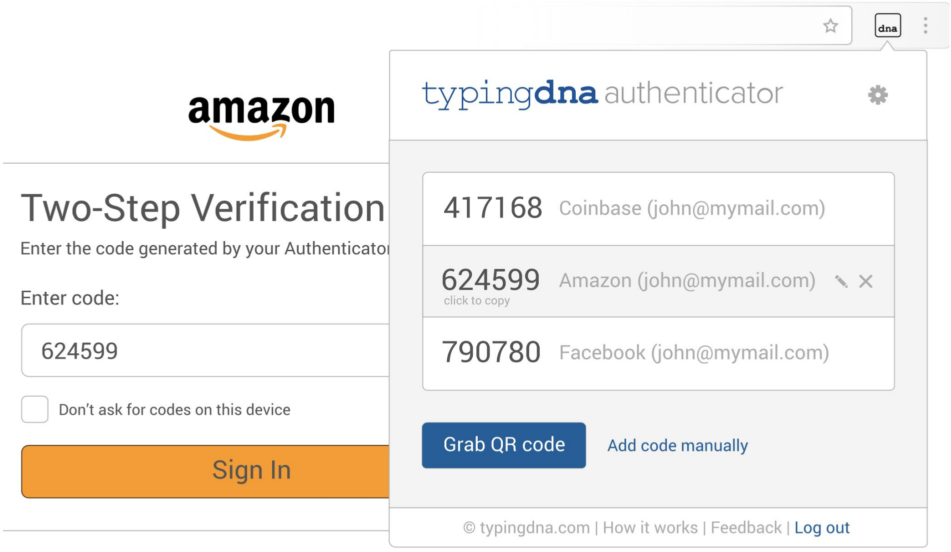
typingdna
Typing Biometrics Authentication

Technical Overview

TypingDNA Authenticator

We recognize people by the way they type

At TypingDNA we use revolutionary AI to replace traditional 2FA with typing pattern authentication, also known as "typing biometrics authentication". Our technology protects against online identity fraud without complicating the user experience. Learn more


amazon

Two-Step Verification

Enter the code generated by your Authenticato

Enter code:

624599

□ Don't ask for codes on this device

typingdna authenticator

417168 Coinbase (john@mymail.com)

624599 Amazon (john@mymail.com)
click to copy

790780 Facebook (john@mymail.com)

© typingdna.com | How it works | Feedback | Log out

About TypingDNA Authenticator

TypingDNA Authenticator is an alternative to Google Authenticator that runs right in your Chrome browser instead of on your phone. It achieves 2FA level security by analyzing your natural typing pattern in the background before producing your OTP 2FA codes.

How it works

Log in with your typing pattern

When you type in your email and password to log in we also look at how you type them. We send your typing pattern to TypingDNA's servers where we match it to previous recordings and return the encryption key.

Grab QR codes, save secret keys locally

Scan the page for QR codes or manually add accounts. All secret keys are stored locally, encrypted with an encryption key that we provide only if you pass the typing biometrics authentication.

One click to paste codes

Simply click an account from the list to copy and paste the OTP code directly into the webpage or other apps.

Why is it safe to use?

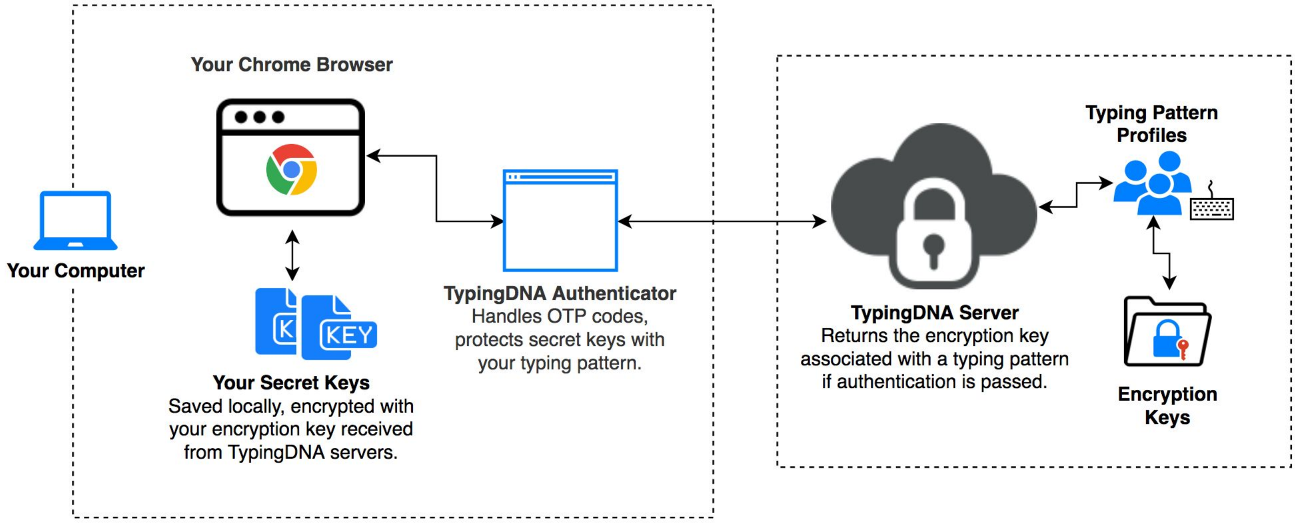
Two reasons. First, only you can log in to the authenticator and get access to your encryption key. Second, your secret keys are stored locally on your PC/chrome account so only you can decrypt your secret keys and produce the 2FA OTP codes needed in other apps.

Vault and authenticator, 2 in 1

Keep all your secret keys safe and sound. Generate your 2FA OTP codes whenever needed and also reproduce the initial QR code for a quick phone rescan.

Is it better than phone authenticators?

The user experience is greatly improved since you don't have to switch devices.


Your Chrome Browser
Your Computer
KEY
Your Secret Keys
Saved locally, encrypted with your encryption key received from TypingDNA servers.
TypingDNA Authenticator
Handles OTP codes, protects secret keys with your typing pattern.
TypingDNA Server
Returns the encryption key associated with a typing pattern if authentication is passed.
Typing Pattern Profiles
Encryption Keys

Achieving 2FA security correctly

For correct 2FA you need to employ 2 different types of factors since every factor class has its weaknesses:

- **Secrets** (what you know, eg. passwords) can be forgotten, phished, stolen & guessed
- **Objects** (what you have, eg. mobile phone) can be lost, stolen, shared, not accessible
- **Biometrics** (what you are, eg. typing biometrics) have FAR, FRR rates & are arguably spoofable

When one factor is compromised, the entire factor class may be at risk.

Is it better than a mobile authenticator?

People don't like to switch devices all the time, also sometimes their mobile phone is not in reach.

Sometimes you need a backup authenticator to use quickly on your computer, a backup that is not protected just with a password since that would not be a correct 2FA from a security perspective.

We suggest storing your accounts/secret keys in both your PC using TypingDNA Authenticator and your phone using Google Authenticator and use whichever is at hand.

FAQ

What do you record in a “typing pattern”?

We record flight & dwell times. The time it takes to reach a key and the time you keep that key pressed. We anonymously store typing patterns, preventing actual typed text from being transferred.

What do you store on my PC?

We store your unique user id, your accounts and your secret keys fully encrypted with the encryption key.

What do you store during an active session?

Once we authenticate you, we throw away your password. We keep the encryption key for a timeout period that you can change from the Settings page. This allows us to produce your 2FA OTP codes, but reduces the ability to perform some actions without re-entering your password (optional to begin with).

What types of encryption do you use?

All secret keys are encrypted with standard symmetric AES encryption. Your password is one way encrypted double hashed (SHA256) and salted for extra protection before it leaves your PC. Your secret keys are saved on your Chrome account based on a hash of your email.

Can I use my account on a different PC/browser?

You can set up an identical account but it won’t be the same one and will not contain your previously saved accounts/secret keys. The user accounts are used locally without any global/sync functionality for the moment. A unique user id is produced when you register a new local user, a user id that is used for typing pattern authentication and for storing your encryption key on our servers.

Can an attacker get access to my encryption key on TypingDNA’s server?

At TypingDNA we’re very strict about this type of data. We never store data such as encryption keys in plain text. We encrypt these with user specific keys and algorithms behind hardware security modules.

Can an attacker get access to my secret keys or 2FA OTP codes on my PC?

Only if you leave your PC and Chrome open, and if you leave your timeout settings long enough so that the encryption key is still present in your active session by the time of the attacker gets to your PC. To prevent this, use a very low timeout setting (Default: 1 hour after last usage).

Connect with us

✉ contact@typingdna.com
@typingdna
in www.linkedin.com/company/typingdna