

WHITEPAPER · V1.0

Midcheck

Spot the lookalike before you send

Address safety 2026-11-03 midcheck.pages.dev

CONTENTS

01 Abstract

02 The problem

03 The solution

04 How it works

05 Design principles

06 Architecture

07 The interactive preview

08 Token and transparency

09 Roadmap

10 Risks and limitations

11 Disclaimer

12 Glossary

01 Abstract

Midcheck is a pre-send address checker. Before a payment, the user pastes the recipient address and Midcheck compares every character with the addresses in the user's history, flagging lookalikes that copy only the first and last characters. It is read-only and never asks for keys.

02 The problem

Attackers seed your transaction history with addresses that copy the first and last characters of ones you use, hoping you copy the wrong one later.

Address poisoning plants a lookalike address in a victim's history, matching the first and last characters of one they use. Wallets show only the ends of an address, so a copied lookalike can pass a quick visual check. Research on Ethereum and BSC found hundreds of millions of such attempts.

Who it is for: Anyone who copies addresses from wallet history or explorers, and teams that pay the same recipients repeatedly.

Why now: A study of Ethereum and BSC found hundreds of millions of poisoning attempts. The trick costs attackers almost nothing and keeps working because wallets show only the ends of an address.

03 The solution

Paste the address you are about to pay. Midcheck compares every character against the addresses in your history and flags near-twins before funds move.

Full-character comparison

Checks every character, not just the first and last few that wallets show you.

History-aware

Compares against addresses you have sent to or received from, including tiny dust transfers.

Read-only

Paste a public address. No wallet connection, no signature, never your keys.

Near-twin alerts

Optional ping when a new lookalike of one of your addresses appears in your history.

04 How it works

1. Paste the recipient: Copy the address you are about to pay.
2. See the diff: Midcheck highlights which characters differ from any lookalike in your history.
3. Send from your own wallet: Pay only once you have confirmed the full address matches.

05 Design principles

- Compare all 40 characters, not just the ends.
- Read-only: a public address is pasted, nothing is signed.
- Show the diff: highlight which characters differ.
- Say what to verify next without scare tactics.

06 Architecture

History reader

Addresses the user has sent to or received from, including tiny dust transfers, are read from public chain data.

Comparator

The pasted address is compared character by character with each address in that history and near-twins are listed with their differences.

Report

The result shows exact matches, near-twins and new addresses, and suggests confirming large payments through a second channel.

07 The interactive preview

The website includes a "Pre-send check" (feed). Simulated events for illustration. Addresses and amounts shown here are made up; real checks run only on addresses you paste.

08 Token and transparency

Midcheck is a software utility. No token launch is described in this version. If a token launches, its supply, every wallet the team controls that holds launch supply, and any locks will be published at https://midcheck.pages.dev/transparency before the launch.

09 Roadmap

Phases describe order, not dates or promises.

Now

- Full-character address comparison
- Near-twin detection against history

Next

- Near-twin alerts
- Address book import

Later

- Team address books
- More chains on request

10 Risks and limitations

- A clean result covers only the addresses visible in the history today and is not a guarantee.
- Lookalike detection can miss an attack that does not resemble any address in the history.
- Coverage depends on public data sources that can be incomplete or delayed.
- The website feed is simulated for illustration; real checks run only on addresses a user pastes.
- Crypto assets are volatile and can lose all of their value.
- Smart contracts, launchpads and other third-party software can contain bugs or change; use of them is at your own risk.
- Data shown by the software depends on third-party sources and may be incomplete or delayed.
- Rules for crypto assets differ by country and can change. Check what applies to you.

11 Disclaimer

This document describes a software utility. It is not financial, legal or tax advice and not an offer to sell or a solicitation to buy any asset. Nothing here promises a return. Information may change; the website is the current source. © 2026 Midcheck.

12 Glossary

Address poisoning

Sending a tiny transfer from a lookalike address so the victim later copies it from their history.

Dust transfer

A very small transfer, often used to plant an address in a history.

Midcheck whitepaper v1.0 · 2026-11-03 · midcheck.pages.dev · Software utility. Not financial advice.