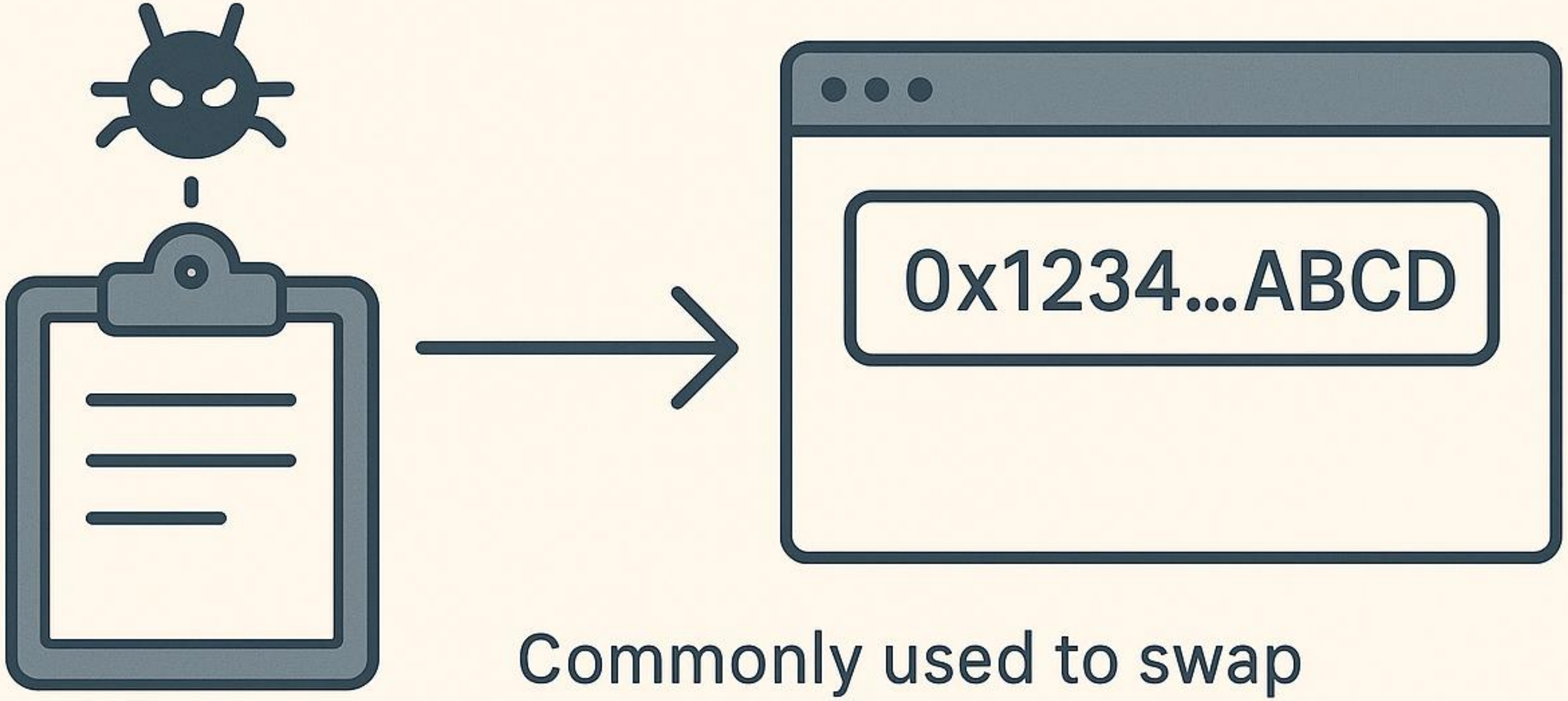
5. CLIPBOARD HIJACKING

Clipboard hijacking is a type of malware that monitors whatever the user copies, such as wallet addresses, payment details, or account numbers, and silently replaces it with attacker-controlled information. This is commonly used to swap cryptocurrency wallet addresses or redirect payments, causing the victim to send money straight to the attacker without noticing the change.

WHAT IS CLIPBOARD HIJACKING?

Malware monitors copied text and replaces it with attacker-controlled data.



Commonly used to swap crypto wallet addresses or payment information

Scenario: Maryam Copies a Wallet Address

Maryam copies her company’s crypto wallet address to send a payment.

When she pastes it, the address looks correct at a glance, but one character has been changed by malware.

The payment is sent directly to the attacker’s wallet instead of the intended recipient.

Clipboard hijacking exploits the trust in simple copy-paste actions.

Lesson: Always double-check addresses character by character before sending funds. Use trusted devices and keep antivirus software updated to prevent clipboard malware.

CLIPBOARD HIJACKING
1A3b1c2D4e5F6
g7H8I9J0
1A3b1c2D4e5F6
g7H8I9J0
Open

How Clipboard Hijacking Works?

- Malware waits in background
- Detects copied text
- Replaces it in milliseconds
- Employee pastes attacker’s value unknowingly

Red Flags Maryam Should Notice

- Pasted value slightly different
- Multiple attempts show different results
- Strange background processes
- Antivirus warnings ignored

Prevention Tips

- Double-check pasted sensitive values
- Keep systems patched
- Use endpoint protection
- Avoid installing untrusted software