bitcoinjenga.com

MILD COLUMN

↓

broadcasting a transaction from the same node that runs your wallet

having a high profile as a public figure or activist

broadcasting a transaction from your home internet

posting pro-bitcoin material on twitter

mixing KYC and non-KYC bitcoin, deanonymizing all UTXOs

talking about bitcoin publicly

attending bitcoin conferences

publicly discussing your personal security practices

using a public blockchain explorer

talking about your bitcoin transactions on an insecure messaging app

sharing widely that you own bitcoin

using the default transaction structure of 1 input & 2 outputs

using one wallet for all purposes

using round amounts when sending payments

using software that doesn't support intentional coin selection

using the bitcoin base layer for all transactions

having bitcoin stickers on your laptop or water bottle

using slightly outdated software

↑

MILD COLUMN

MODERATE COLUMN

↓

linking Lightning node pubKey to your public identity

spending funds from a dust attack

sharing how much bitcoin you own

installing suspicious browser extensions

sharing screenshots of wallets with identifiable information

delivering bitcoin hardware to your home address

logging into wallet or exchange from a public, shared computer

combining inputs from many UTXOs into a single transaction

reusing an address for a second transaction

using a software wallet that fingerprints all transactions

using a compromised block explorer

using extremely outdated software

publicly sharing about tax evasion

creating unique and identifiable transaction structures

storing your private keys in the cloud

using an app that allows SMS password retrieval

posting to twitter complaining that your transaction hasn't been mined for x amount of minutes

broadcasting a transaction from your home IP address

↑

MODERATE COLUMN

SEVERE COLUMN

↓

sharing the location of your bitcoin private keys

tweeting about engagement in illicit activity

putting your bitcoin address on your business card

posting your bitcoin address on your website for donations

tweeting an image of your transaction

using a compromised ISP

spending KYC bitcoin

using a compromised wallet

using public bitcoin APIs that log your data

selling bitcoin on a KYC exchange

inputting private information into a phishing attack

publicly sharing your IP address

sending your bitcoin to a malicious entity

putting identifiable information in an OP_RETURN

exclusively using exchanges to manage all transactions

repeatedly reusing the same address

submitting your private keys to a malicious software wallet

storing your private keys in a browser extension

↑

SEVERE COLUMN

bitcoinjenga.com