The Truth in the Data: The 15-Point Digital Deception Checklist

A Practical Guide to Spotting Hidden Digital Tracks

PRESENTED BY TRUSTED PRIVATE INVESTIGATORS | TRUSTEDPI

FOREWORD: Thinking Like the Attacker

By Lavi Peretz | Head of Offensive Security (Red Team)

In the cybersecurity world, my name—Lavi—means "lion." For years, I've operated as a white hat hacker, hunting for vulnerabilities and developing zero-day exploits before malicious actors can find them. My job is to think like the attacker. I look at systems, networks, and devices to find the invisible cracks that people use to hide, infiltrate, or steal.

At Trusted Private Investigators | TrustedPi, my elite technical team and I apply that exact same offensive security mindset to digital forensics.

Whether someone is hiding illicit financial assets, covering up a secret life, or trying to erase their tracks, they always leave a digital footprint. Modern devices are built to record our lives, which means true digital deletion is incredibly difficult. If you know what to look for, the deception becomes glaringly obvious.

This 15-point checklist is designed to help you trust your gut. We've stripped away the complex tech jargon to give you a human, straightforward guide to the red flags of digital deception.

📱 PHASE 1: Device Behavior & Access

The first signs of deception usually start with how a person interacts with their physical device.

1 The "Fort Knox" Pivot

It's not just that they have a passcode; it's that the passcode suddenly changed, FaceID/TouchID was disabled, and the phone never leaves their physical possession. If they take the phone into the shower or sleep with it under their pillow, they are guarding a perimeter.

2 The Phantom Battery Drain

Does their phone battery constantly die at 2 PM? While it could just be an old battery, severe and sudden battery drain is a primary symptom of hidden background processes—like encrypted vault apps, secondary location spoofers, or even consumer-grade spyware running constantly.

3 Autocomplete Betrayals

Smartphones are designed to learn from us. If you casually borrow their phone to search for something, pay attention to the predictive text or search bar history. If the keyboard suggests unusual names, unvisited cities, or strange crypto-exchange URLs when typing a single letter, the phone is remembering what the user is trying to forget.

4 The "Second Device" Disguise

Finding a physical burner phone is rare these days. Instead, look for digital burners: apps like Google Voice, TextNow, or Burner that generate secondary, untraceable VoIP phone numbers straight from their primary smartphone.

💬 PHASE 2: Applications & Communications

How people talk, and where they hide those conversations.

---

5 Vault Apps and "Calculator" Disguises

Not every calculator app is just a calculator. Look for generic-looking utilities on the phone (calculators, audio managers, or note apps) that require a PIN to open. These are often "vaults" designed to hide photos, videos, or documents securely away from the main camera roll.

6 The Disappearing Act (Ephemeral Messaging)

Apps like Signal, Telegram, and WhatsApp are fantastic for privacy, but they are also the gold standard for deception. If they have "disappearing messages" turned on—where texts auto-delete after 1 hour or 24 hours—they are ensuring no digital forensics team

can easily recover their conversations without advanced tools.

7 Obsessive Digital Housekeeping

Normal people rarely clear their browser cache, delete their text message threads daily, or constantly empty their "Recently Deleted" photo album. If their digital trash cans are always spotless, it's a manual, intentional effort to destroy evidence.

8 Hidden Home Screens & App Libraries

Both iOS and Android allow users to completely hide entire pages of apps from their home screen. An app might be installed on the phone, but you will only find it by searching the phone's deepest App Library or looking at their App Store download history.

💰 PHASE 3: Financial Obfuscation & Digital Assets

Money leaves a trail, even when it's not physical cash.

---

9 The Cryptocurrency Black Hole

We frequently investigate cases where stolen or hidden wealth is funneled into digital assets. Look for apps like Coinbase, Kraken, or Binance. More importantly, look for "cold wallet" apps (like Trust Wallet or MetaMask) or physical USB devices (Ledger, Trezor). If they are heavily invested in crypto but the bank statements don't reflect it, money is being hidden on the blockchain.

10 Expense Masking via Cash Apps

Venmo, CashApp, and Zelle are convenient, but they are also great for hiding the true nature of a transaction. If you see large, unexplained transfers to seemingly random usernames, or frequent purchases of digital gift cards, it's a classic method of laundering personal funds to be spent invisibly elsewhere.

11 Unexplained Cloud Storage Upgrades

Are they paying a monthly subscription for extra Dropbox, Google Drive, or Mega.nz storage, but their main computer is empty? Secret cloud accounts are the modern filing cabinets for hidden documents, illicit financial ledgers, and illicit media.

📍 PHASE 4: Location, Routine, and Network Anomalies

Where they are, and what networks they connect to.

---

12 Location Spoofing and "Dead Zones"

If you use location sharing (like Find My Friends or Life360) and their phone routinely says "Location Not Available" or shows them sitting at the office while they are unreachable, they might be using location-spoofing software or intentionally turning off their GPS modules.

13 The Saved Wi-Fi Network Trail

A smartphone automatically saves and logs the names (SSIDs) of every Wi-Fi network it successfully connects to. If you look in their Wi-Fi settings and see connections to "Marriott-Guest," a specific apartment complex, or an unknown cafe across town, their phone is proving they were there.

14 Constant Incognito or Alternative Browsers

Using Chrome's "Incognito Mode" occasionally is normal. Using an alternative browser like DuckDuckGo, Brave, or Tor exclusively for certain sessions—and never saving bookmarks or history—shows a dedicated effort to evade basic digital tracking.

15 The Two-Factor Authentication (2FA) Burner

If you notice an authenticator app (like Google Authenticator or Authy) on their device with codes for accounts you don't recognize (like a secret Instagram account, an unknown email, or an offshore crypto exchange), you have definitive proof that hidden accounts exist.

🔎 WHAT NOW?

Finding one or two of these signs might be a coincidence. Finding a cluster of them means there is a systematic effort to deceive.

When your gut tells you the truth but the data is being hidden, don't confront the issue blindly. Confrontation often leads to the immediate destruction of the remaining evidence.

That's where we step in. At Trusted Private Investigators | TrustedPi, Lavi Peretz and our elite technical team use advanced digital forensics to recover deleted data, trace hidden crypto assets, and uncover the truth that standard methods miss.

Don't guess. Know. Contact TrustedPi today for a confidential consultation.
