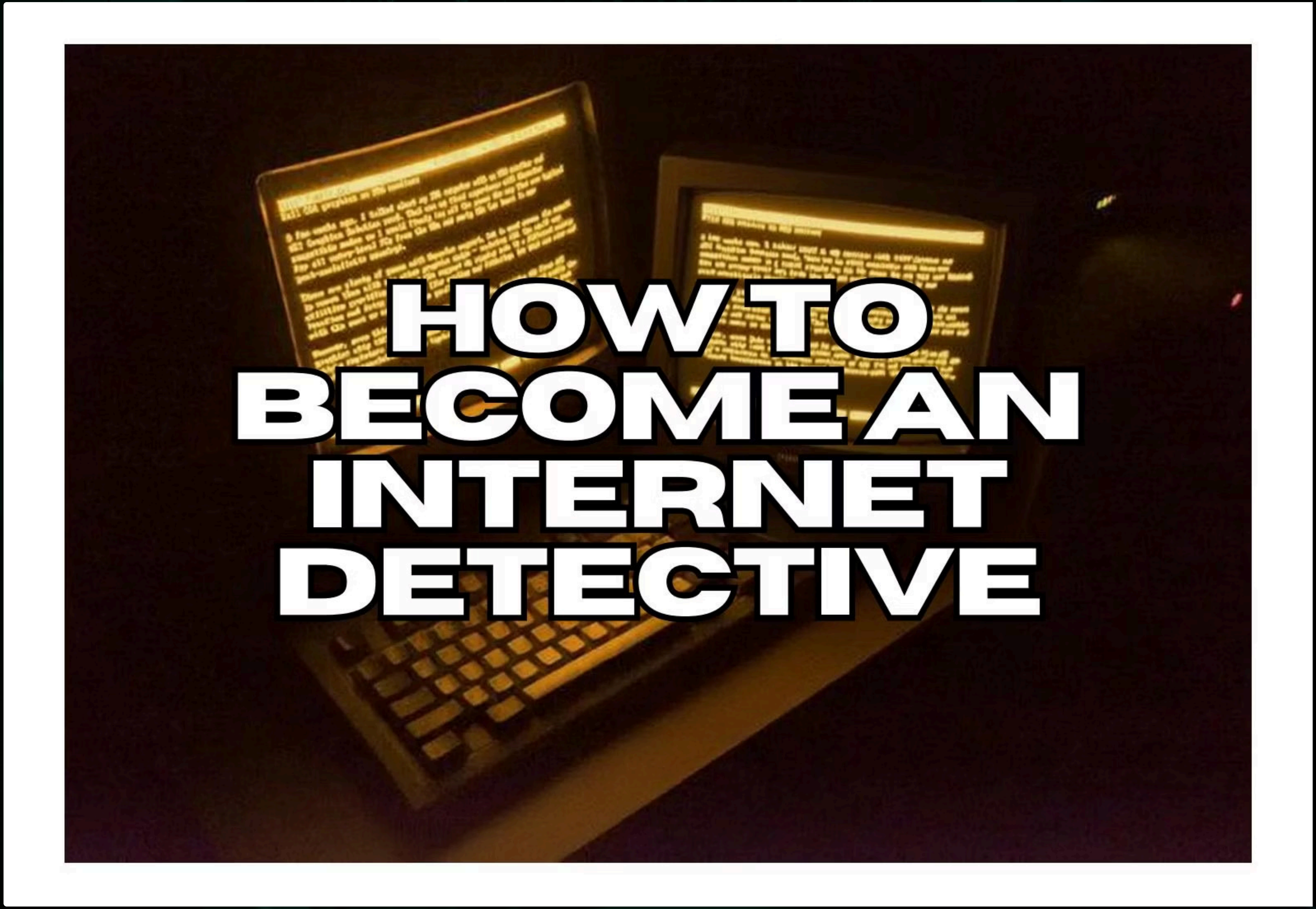
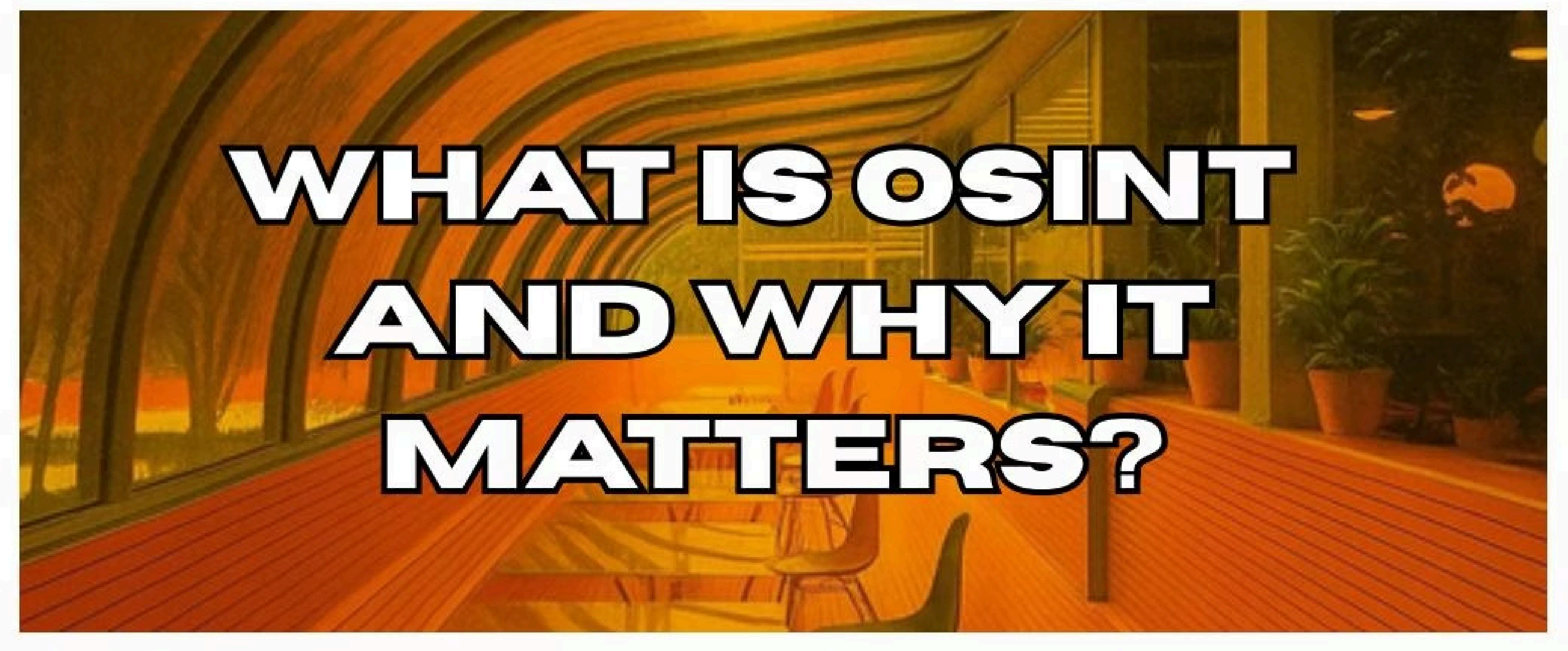
OSINT INVESTIGATIONS



Introduction

Welcome to this fast-paced guide to uncovering hidden information online. Learn how to run background checks, trace digital footprints, spot scams, and remove your personal information before it's stolen.



Open Source Intelligence, or OSINT, refers to collecting and analyzing public information for investigative or security purposes. Unlike hacking, OSINT uses what's freely accessible: websites, public records, social media and much more.

A huge amount of your data exists on the internet. Old and forgotten accounts, employee or LinkedIn profiles, and public court records. Most people leave digital footprints that can be traced, cross-referenced, and analyzed -often extremely accurately.

Who Uses OSINT?

OSINT is used daily by:

- Private Investigators tracking down subjects
- Journalists uncovering connections and verifying sources
- Cybersecurity experts mapping out potential flaws
- Law enforcement conducting background research
- Scammers and stalkers looking to exploit personal information

Understanding OSINT is a modern survival skill. Whether you're dating online, vetting a job offer, checking who's behind a phone number, or securing your digital presence, knowing OSINT basics gives you a huge advantage.

In the pages ahead, we'll cover:

- How to perform safe and legal digital investigations
- The best tools (mostly free!) for tracking people, places, and accounts
- How to see what others can find about you—and how to hide it

Legal and Ethical Considerations

One of the most common misconceptions about OSINT is: "If it's online, it's fair game." This isn't true.

Fair Game vs. Snooping

Open Source Intelligence refers to using publicly available data. This includes:

- Public social media profiles
- Government or public records
- Search engines and forums
- News articles and databases

However, certain actions cross into illegal territory:

- Accessing private accounts or password-protected data
- Posing as someone else to gain access (social engineering)
- Using scraped data in ways that violate terms of service
- Attempting to blackmail or extort using gathered information

Remember this key principle: If you have to trick, hack, or force your way in-it's not OSINT. It's illegal.

The Ethics of OSINT

When investigating someone:

- Ask yourself: Why am I doing this? Is it for safety, curiosity, or revenge?
- Don't dig just to "see what's there"—have a clear, justifiable purpose.
- Never post, share, or weaponize private findings (blackmail)—especially addresses, photos, or family connections.

When investigating yourself:

• Use what you find to strengthen your digital presence.

Apply this knowledge to clean up and secure your information.

Staying Safe and Clean

To remain legal and ethical:

Stick to publicly available information

Respect platform terms of service

Don't impersonate or manipulate people

Avoid sharing PII (personally identifiable information) of others

Never monetize findings in ways that harm others

OSINT can protect and empower. But when misused, it can easily harm or even criminalize. Let this chapter serve as your ethical compass before diving deeper.

Investigation Methodology

Investigating someone online can seem like a lot at first, but with an organized approach, you can uncover a surprising amount of information. Whether you're checking a suspicious caller, vetting a potential date, or examining your own digital footprint, begin with the information you already have.

Step 1: Start with Known Data Points

Every OSINT investigation begins with seed data—basic details you already have. Examples include:

- ***Full name, or partial***
- ***Email address***
- ***Phone number***
- ***Usernames***
- ***Social media accounts***
- ***A photo or video***

Just a single data point can unlock a wealth of information. Your goal is to pivot from one piece of information to another.

Step 2: Pivot, Cross-Reference, Repeat

Think like a detective. If you have a username, search it on:

- ***Instagram, TikTok, Twitter/X, Reddit, YouTube***
- ***Username search tools (Namechk, whatsmyname, etc.)***
- ***Google (with quotes and modifiers like site: or onpage:) examples can be found here, this method is called "Google dorking" and can be incredibly useful.***

Each new piece of info branches into new leads. Cross-check everything for consistency and context. For example, a Reddit post might reveal an email, which connects to a LinkedIn profile, which leads to a workplace.

Step 3: Use the Right Tools

Here are specific tools for different types of data:

- ***Names & usernames: Namechk, BeenVerified, Spokeo, EnfomionGO***
- ***Emails: Emailrep.io, HaveIBeenPwned, Dehashed, pentester.com (paid)***
- ***Phone numbers: TrueCaller, Sync.me, NumLookup, OSINT Industries (paid)***
- ***Photos: Google Lens, Yandex Images, ExifTool (for metadata)***
- ***Social media: Social Searcher, WhoPostedWhat, Archive.org***

Always document your findings with screenshots and notes.

Analysis and Boundaries

Step 4: Analyze Behavior, Patterns, and Connections

Don't just collect data—understand it. Think:

- Does this person maintain a consistent online identity?
- Can you identify their friends, relationships, or group affiliations?
- What patterns emerge from their posts, bios, or activity timestamps?
- Are there inconsistencies in how they present themselves?

Behavioral analysis often reveals more than the data itself.

⚠️ Step 5: Know When to Stop

Don't venture too deep out of mere curiosity. Respect privacy boundaries. Stop when:

- You've found what you need
- You're encountering sensitive or private information

Remember: This is about empowerment, not obsession.

Essential OSINT Tools

You don't need a budget to start doing effective OSINT. Many free tools can reveal everything from photos to second identities. In this chapter, we'll explore tool categories, what they do, and where to find them.

People Search Engines

These tools collect public data from multiple sources, including names, phone numbers, emails, addresses, and possible relatives:

- **TruePeopleSearch** – Great for U.S. addresses and relatives
- **FastPeopleSearch** – Similar results, mobile-friendly
- **Pipl** (limited free access, paid version is deeper)
- **PeekYou** – Finds online aliases and web mentions

Tip: *Cross-verify results between multiple sites. False positives are common.*

Social Media Discovery Tools

People reveal a lot online. These tools help locate public social accounts:

- **Namechk** – Check username availability across dozens of platforms
- **WhoPostedWhat** – Search public Facebook posts by keyword + year
- Social **Searcher** – Tracks mentions, hashtags, and public posts
- **PublicWWW** – Find email addresses or code snippets in public HTML

Email & Phone Lookup Tools

Need to trace a number or verify an email? Start with these tools:

- ***HaveIBeenPwned*** *– Checks if an email has appeared in a data breach*
- ***EmailRep.io*** *– Gives reputation score + linked domains*
- ***NumLookup*** */* ***Sync.me*** *– Caller ID and reverse phone lookup*
- ***That's Them*** *- Multi-data search: phone, IP, email, and address*

Don't forget to reverse-search numbers in Facebook, CashApp, and Telegram-they often link to real profiles.

Browser Plugins & Helpers

These add-ons streamline your workflow:

Exif Viewer

Extract metadata from images

Reveye / Google Lens

Reverse image searches from right-click $\bullet$

SingleFile (Chrome)

Save entire web pages for later analysis

Lightshot or GoFullPage

Take full screenshots to log findings

Always keep a record. Use a private doc, folder, or tool like **Obsidian**/**Notion** to track every piece of info.

Advanced Investigation Techniques

After gathering the basics—it's time to dig deeper. This chapter teaches you how to build timelines, uncover past records, and spot inconsistencies. These methods are great for background checks, and due diligence.

Timeline Building: What Happened, When?

One of the most overlooked aspects of OSINT is time-based correlation. Try to:

- Match social media posts to life events
- Compare profile creation dates
- Use archive tools (like Wayback Machine) to view past versions of web pages
- Log job changes, moves, and aliases by year

Free tools like Web Archive, Google Dorks, and Social Blade help you establish a digital trail.

Public Records and Court Databases

Depending on the country or state, a wealth of public information is available:

- Local court systems – Civil, criminal, and traffic records
- County assessor sites – Property ownership and transfers
- State licensing boards – Check for business, real estate, contractor licenses
- PACER (U.S. Federal court records – paid)

Look for:

- Lawsuits or restraining orders
- Bankruptcy or liens
- Prior addresses or business ties

Work History and Verification

Work and Education History

Many people exaggerate credentials. To verify:

- Check LinkedIn, resume PDFs, and old bios
- Search with "Name" AND "University" or "Name" AND "Job Title" on Google

OSINT doesn't guarantee truth—it shows what people claim. Verification is key.

Connecting Online Aliases

Digital footprints often leave traces across accounts. To find and connect them:

- Match writing style, emoji use, and slang
- Reverse search unique profile pictures
- Look at username similarities and reused bios
- Use Username checks across niche forums, marketplaces, and alt platforms

If someone uses the same avatar on a Reddit post and a gaming profile, you've likely found a connection between aliases.

✅ Verification Techniques

Before drawing conclusions:

🌐 Cross-reference every claim with at least 2+ sources

🌐 Use archived versions when current data is missing

🌐 Save and document your findings with timestamps

Misinformation, outdated data, and intentional misdirection are common online. Careful verification separates a solid OSINT report from a flawed one.

Next, we'll shift gears—toward protecting yourself from the very techniques you've now learned.

Investigating Yourself

> *Now that you know how to investigate others, it's time to turn the lens inside. Understanding what's publicly accessible about yourself can be eye-opening—and sometimes unsettling. This awareness is the first step toward true digital privacy.*

What Can Be Found About You?

To start, run a basic OSINT sweep on yourself:

- Google your full name in quotes: "Johnathan M. Doe"
- Add keywords like your city, workplace, or school
- Check for old usernames, accounts, and photos
- Search your phone number and email using people search engines

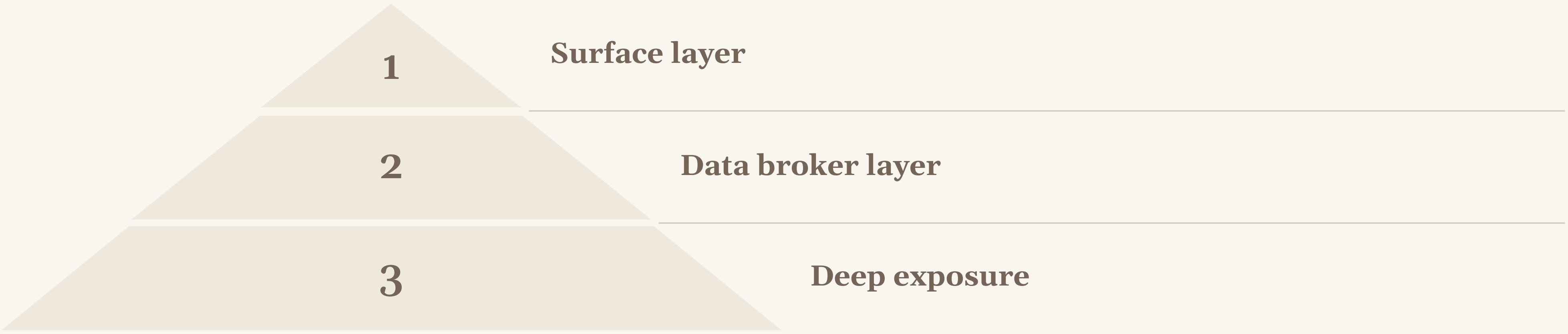
You'll likely uncover:

- *Social media profiles (active and abandoned)*
- *Forum posts, blog comments, or photo tags*
- *Public records (addresses, voter registration, property ownership)*
- *Breached data tied to your accounts*

Digital Exposure Layers

Layered Exposure

Your digital footprint exists in layers:



1 Surface layer

2 Data broker layer

3 Deep exposure

1. Surface layer – *Search engines and active social profiles*
2. Data broker layer – *Combined info from marketing firms and search sites*
3. Deep exposure – *Breached credentials, exposed documents, old archives*

Each layer requires different tactics to identify and clean up.

Use the same tools investigators use—just flip the perspective:

- HaveIBeenPwned – See if your email was in a data breach
- Namechk – Find old accounts from reused usernames
- Whitepages / Spokeo / EnformionGO – Preview what others might see
- Google Dorks – Use advanced search operators to dig deeper (e.g., intext:"YourName" filetype:pdf)
- Wayback Machine – Look at old versions of your online footprint

Risk Assessment and Clean-Up

What to Watch For

Pay attention to:

- Doxxing risk factors: Addresses, school names, family links
- Security exposure: Passwords reused across accounts
- Reputation risks: Old social media posts, forum comments, photos

Document your findings and prioritize based on risk: what would cause the most damage if someone weaponized it?

✅ Clean-Up Begins With Awareness

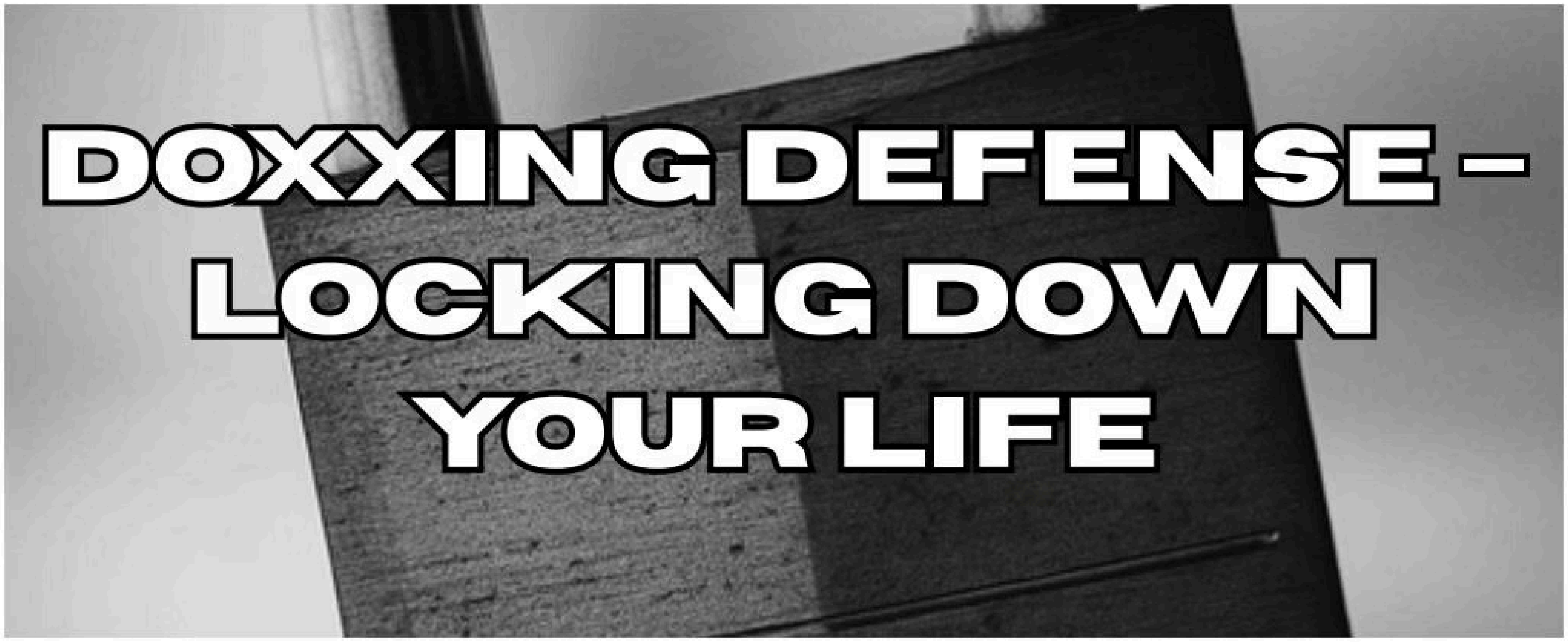
You can't clean everything—but you can reduce your exposure:

- Remove or update old bios and accounts
- Use opt-out forms for data broker sites (see next chapter)
- Adjust privacy settings across social media
- Consider changing usernames and rotating email aliases going forward

This self-audit is a mirror. The better you understand what's visible, the better you can protect it.

Next: Let's go on defense—doxxing protection and locking your data down.

Doxxing Protection



Doxxing—the exposure of your private information online—has evolved from an internet tactic into a mainstream weapon. It's now used in everything from online feuds to political intimidation. How easily could someone find your personal details if they looked?

In this chapter, we'll explore how to secure your data before someone else weaponizes it against you.

Start With the Big Targets: Address, Phone, and Email

These three pieces of information are the holy grail of doxxing. Here's how to protect them:

Phone numbers

Use a **Google** Voice number or VoIP service for public-facing accounts. Never reuse your personal number on domains, accounts, or WHOIS data (signing up for websites).

Email addresses

Use different emails for different purposes—personal, business, newsletters, and logins. Consider aliases or masked email tools like **SimpleLogin**.

Home addresses

Remove from data broker sites (see next section). Keep your address off all social media bios and posts.

Bonus: Use a UPS box or virtual mailbox for deliveries and registrations.

Data Broker Opt-Out

Opt-Out of Data Brokers and People Search Engines

Companies collect and sell your personal data. Here's how to start removing it:

Find Opt-Out Links

Use **mydataremoval.com** to find direct opt-out links

Request Removal

Request removal from sites like **Whitepages**, **Spokeo**, **MyLife**, **PeopleFinders**

Consider Automation

Consider tools like **DeleteMe**, **Optery**, or **OneRep** for automation, or do it yourself for free

Make this a habit—most sites re-add your data after 30–90 days.

Social Media Lockdown

Privacy Settings

Set profiles to private (especially Facebook, Instagram, TikTok)

Location Data

Remove location tags from photos

Content Audit

Delete or archive old content that reveals life patterns or family connections

Tagging Policy

Avoid tagging your home, school, or close contacts in public posts

OSINT-savvy actors often trace people through friends and tagged content.

Extra Layers of Protection

- **Register domains with WHOIS privacy protection**
- **Use pseudonyms (fake names) for non-public-facing accounts**
- **Run reverse image searches on your own photos to see where they appear**
- Regularly audit your online presence using Google and OSINT tools

Responding to Doxxing

What If You're Targeted?

If someone starts posting your information, take these steps:

Document everything

Screenshots, links, timestamps

Report to platforms

Most major sites have privacy violation processes

File a police report

Especially if threats or harassment are involved

Use takedown services

DMCA requests or professional help for content removal

Lock down accounts

Change passwords, enable 2FA, remove unnecessary links

The best defense is preparation. You don't need to disappear completely—just make yourself harder to target.

Next, we shift gears. You've learned how to investigate and how to protect yourself. Now, let's explore how OSINT is applied in real-world scenarios.

Real-World OSINT Applications

OSINT isn't just for large investigations—it's a powerful everyday tool. Whether you're meeting someone new, hiring help, or buying from a stranger, the internet leaves a trail that can help you make safer, smarter decisions. This chapter highlights common real-life situations where OSINT can add an extra layer of protection.

Online Match Verification

Scenario: *You've matched with someone new and want to ensure they are who they say they are.*

Approach:

- **Search their name, username, or phone number in Google and social platforms.**
- **Use reverse image search to check for reused or fake photos.**
- **Scan for inconsistencies in stories, multiple profiles, or conflicting timelines.**

Tools: Namechk, SocialCatfish, PimEyes, Google Dorks (cheat-sheet here)

Insight: A little pre-check can spare you emotional or even financial fallout. If the profile is real, it'll hold up. If not, you'll likely find cracks.

Scam Prevention and Vetting

Scam-Proofing Sellers and Listings

Scenario: You're buying from Craigslist, Marketplace, or booking an Airbnb.

Approach:

- Check the email or phone for scam reports.
- Reverse search product images and descriptions.
- Use Street View to confirm a real location behind a rental or listing.

Tools: Google Lens, Whois Lookup, Reddit, Trustpilot

Insight: If you find the same images on stock sites or the property on multiple platforms with different names—it's probably a scam.

Vetting Clients, Coworkers, or Freelancers

Scenario: You're about to sign a contract, take a freelance gig, or work with a new client.

Approach:

- Look up the business, their domain age, and online presence.
- Verify employment via LinkedIn or company directories.
- Use email rep checkers to verify digital credibility.

Tools: SignalHire, Hunter.io, EmailRep.io

Insight: Trust but verify. If someone's offering great money with little background or referenced work, be cautious.

Trust Your Instincts

When Something Feels Off

OSINT delivers data, but judgment makes the call. Red flags may include:

Avoidance of video calls or public meetups

Inconsistent or vague backstories

Urgency, emotional pressure, or unexpected asks for money

Approach: Pair intuition with investigation. Look for confirmation—not just comfort.

In the final chapter, we'll explore how to stay sharp in the evolving OSINT landscape, with communities, tools, and training to keep your skills fresh.

Staying Current with OSINT

The tools and methods you've learned in this book are powerful—but the world of OSINT doesn't sit still. Laws evolve, and new tools pop up constantly. Staying sharp is what makes a truly skilled investigator.

This final chapter is your guide to continuous improvement in the OSINT space.

Join Active OSINT Communities

Being part of a community keeps you up-to-date and connected.

Reddit

r/OSINT, r/Privacy, r/ThreatIntel

Twitter/X

Follow tags like #osint, #infosec

Discord

Many OSINT Discord servers share alerts, tools, and methods in real time

Slack

Some infosec groups host OSINT-specific threads

These spaces are where professionals and hobbyists share breaking methods, new leaks, and case studies.

Resources and Maintenance

Follow Newsletters and Blogs

A few standout resources that bring fresh info:

- OSINT Curious – Weekly updates, tool breakdowns, and tutorials
- Bellingcat – Investigative journalism powered by open-source techniques
- The OSINT Dojo – Training, guides, and community shoutouts
- Sector035's Week in OSINT – Excellent roundups of the latest resources

Blogs often post walkthroughs that show how real investigations unfold using public data.

Watch and Learn

YouTube is packed with free training content:

- Search for topics like "OSINT for beginners" "How to find someone online" or "Open-source tools demo"
- Follow creators who walk through real cases step-by-step
- Use playlists to stay consistent with learning

Many professionals also livestream their methodology—great for picking up new tricks.

Keep a Personal OSINT Toolkit

Organize your favorite tools into a personal database or Notion board. Include:

- Bookmarked links
- Saved searches
- Templates for investigations or reports
- Ongoing cases

Keeping everything in one place means you can jump into action without wasting time setting up.

Revisit Your Own Exposure

At least twice each year, re-run your personal digital audit:

- What's changed about your online presence?
- Are there new data breaches?
- Is your opt-out status still active?

Think of your digital footprint like a garden—if you don't maintain it, it gets overgrown.

Final Words

You now have the skills to dig deeper, verify smarter, and protect yourself in ways most people can't. OSINT gives you an edge—not to exploit, but to stay aware, resilient, and informed.

Stay curious. Stay ethical. And keep watching the watchers.