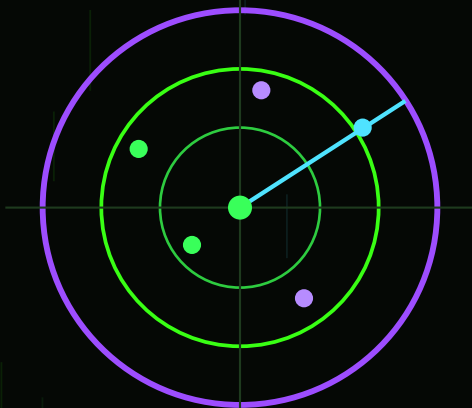




OSINT

LIVE CONNECTIONS VIEWER

The free keys that turn on the deep checks —
where to get them, how to add them, how to use them.

[GETTING YOUR KEYS](#)

KEYS GUIDE · OCTOBER 2026

777 SOFTWARE

FREE — AND IT STAYS FREE

1 — WHY KEYS AT ALL?

OSINT works the moment you open it. The board fills with your live connections, the known-bad lists are checked against them, and every row gets a plain-words verdict. You do not need any key for any of that, and there is no account to make — not with us, not with anybody.

What a key adds is depth. Four outside services each keep a different kind of memory about internet addresses — who has been reported for abuse, what dozens of scanners think, whether an address is part of the internet's background noise, whether a host has served malware links. Each service will give you a free personal key — a short secret line of text — and when you paste that key into OSINT, the app can ask that service about the addresses on your board, in your name, on your allowance.

Every key in this guide is free, straight from the service itself. If a page ever asks you for a card, you are on the wrong plan — close it and take the free one named in the steps.

Service	What it answers	Key needed?
VirusTotal	How many security scanners flag this address	Yes — free key turns its button on
AbuseIPDB	Has this address been reported for abuse, and how strongly	Yes — free key turns it on (then it runs by itself)
abuse.ch — URLhaus	Has this host served malware links	Yes — free Auth-Key turns its button on
GreyNoise	Background internet noise, or aimed at you	No — works without one; a key only raises the allowance

Your keys are yours. OSINT stores them in one settings file on your own computer, locked to your own account. They are never uploaded, never sent to 777 Software, and never included in any download. When a check runs, the app sends the address being checked — and your key — to that key's own service, and nowhere else. That is the whole arrangement, and §6 shows you exactly where the keys go.

2 — VIRUSTOTAL

What it answers: dozens of security scanners vote on an address. OSINT shows their count in plain words — how many say malicious, how many say suspicious, how many say harmless.

Where to go: virustotal.com

1. On the VirusTotal home page, choose Join us to start a free account.
2. Fill in the form: your first name, last name, email address, a username, and a password. (They also offer a Google sign-in — the written form works the same.)

3. Pass the "I'm not a robot" check and send the form. The page answers "Signed up successfully."
4. Open the email they send you and click the activation link. Without this click the account stays asleep.
5. Sign in. Open your profile menu and choose the API key page — your personal key is shown there.
6. Copy the whole key. §6 shows you where it goes in OSINT.

The free tier: a standard free account. The API key page says so, and the free public allowance is 500 lookups a day — far more than a person checking connections by hand will ever use.

One honest note, in VirusTotal's own spirit: any address checked through their API is added to the VirusTotal dataset and can be seen by their community. OSINT says the same thing right in its Settings, next to the VirusTotal field. If that trade doesn't suit you, leave the field empty — the rest of OSINT works without it.

3 – ABUSEIPDB

What it answers: has this address been reported for abuse — spam, attacks, scanning — and how confident is the crowd? OSINT shows it as an abuse confidence score out of 100, with the number of reports. Of the four keys, this is the one the app itself calls the best "has this address been reported misbehaving?" score.

Where to go: abuseipdb.com

1. Choose Register and pick the Individual FREE plan. Free means free — no card, ever.
2. Fill in your first name, last name, email address, and country, registered as an Individual. The username box can stay empty.
3. Set your password and pass the "I'm not a robot" check. The site answers: "Your account has been created."
4. Verify your email before anything else. Open the verification email they send and click its link. The Keys page stays locked until you do — this is the step everybody misses.
5. Back on the site, open your Account, then API Keys. Create a key (the name is up to you — "My App" is fine).
6. Press Show to reveal the key and copy the whole thing. §6 shows you where it goes in OSINT.

The free tier: the Individual plan is free forever — 1,000 checks and reports — and the register page says so in plain words before you sign up.

No button to press later: once your AbuseIPDB key is saved in OSINT (§6), the app runs this check by itself for the outside addresses on your board. Its answer appears in the detail pane under WHAT THE CHECKS SAID, on the AbuseIPDB line — score, reports, and when it last spoke.

4 — GREYNOISE

What it answers: is this address part of the internet's background noise — the endless scanning that washes over everybody — or is it something rarer? GreyNoise also keeps a set of known-benign services, so a famous, well-behaved address reads as exactly that.

Where to go: greynoise.io

1. Choose Sign Up and take the free Personal email option.
2. Enter your email address and set a password.
3. Complete your profile — first name and last name (the title box can stay empty). The site won't open the rest until this is saved.
4. Click the verification link they email you. Your free account is now live.

Now the honest part — read this before hunting for a key: a personal-email account does not include an API key. GreyNoise says so on the account's own page: keys are given to work-email accounts. That is their rule, and there is no free-key page hiding somewhere that you missed.

And the good news: OSINT doesn't need one. The Check with GreyNoise button works with no key at all, inside a small free daily allowance. When the day's allowance is spent, the pane says so in plain words — “Free allowance used up — press the button again tomorrow” — and every other check keeps working.

If you do have a work email (your own company or organization address — not Gmail): you may make a GreyNoise account with it, and that account does come with a key, shown in its account settings. Paste it into OSINT the same way as the others (§6). All it buys is a little more allowance — the app itself puts it plainly: a key “raises the tiny free GreyNoise allowance a little” (free keys run to about 50 lookups a week). Nobody needs it; it is there if you ever want it.

5 — ABUSE.CH (THE URLHAUS KEY)

What it answers: abuse.ch runs URLhaus, a list of hosts caught serving malware links. OSINT asks: has this host served malware links? A yes here is a loud answer — the pane shows a warning line naming the threat.

Where to go: auth.abuse.ch — the sign-in house for abuse.ch.

1. Type your email address into the sign-in link by email box.

2. Pass the “Verify you are human” check — a real person passes it in a second; it is there to keep robots out of a free service.
3. Press “Email me a sign-in link.”
4. Open the email that arrives and click its sign-in link. There is no password to invent — the link is the key to the door.
5. Your profile page shows your Auth-Key. Copy the whole thing. §6 shows you where it goes in OSINT — into the field labeled abuse.ch Auth-Key.

The free tier: an abuse.ch account is free. The Auth-Key on your profile is the only credential OSINT needs from them.

6 – PUTTING YOUR KEYS INTO OSINT

Same road for every key. Do it once per service, in any order, whenever you get each key — OSINT does not need all four, and each one turns on the moment it is saved.

1. Open OSINT.
2. Press the Settings button (bottom bar). The OSINT — Settings window opens.
3. Find the field for your service. The window shows four, in this order: AbuseIPDB key, VirusTotal key, abuse.ch Auth-Key, GreyNoise key. Each field hides what you type behind dots, and under each one the app reminds you: “Key saved on this computer only.”
4. Paste the whole key into its field — no spaces at the start or end.
5. Press Save Settings. The window answers: “Saved — on this computer only.” That is done — the key stays saved across restarts; you do not paste it again.

The field names, matched to §2–§5:

VirusTotal key (§2) → the VirusTotal key field

AbuseIPDB key (§3) → the AbuseIPDB key field

GreyNoise key (§4, work-email accounts only) → the GreyNoise key field

abuse.ch Auth-Key (§5) → the abuse.ch Auth-Key field — this is the key that turns on the URLhaus check

The product truths, plainly

- Save means saved. Save Settings writes every field in the window — permanently, until you change it.
- One file, your computer, your account. The keys live only in OSINT's local settings file, locked so only your own user account can read it (file permissions 0600). The file is never uploaded anywhere and is never part of any download.
- A key is a secret. Treat it like a house key: don't post it, don't message it around, don't paste it into web pages that ask out of nowhere. The only places it ever goes are the service that issued it and OSINT's Settings field.

- Removing a key: open Settings, clear the field, press Save Settings. That check turns back off (for GreyNoise, the button simply returns to its free keyless allowance).
- Changing a key: paste the new one over the old and Save. Done.

7 – RUNNING THE CHECKS

1. On the board, click one connection. The detail pane under the board shows that connection — who it is, and what the checks said about it.
2. Under the pane sit the check buttons: Copy IP, Check with GreyNoise, Check with VirusTotal, Check with URLhaus. Press the one you want.
3. The pane tells you the check is running, and its answer lands in the same pane, under WHAT THE CHECKS SAID.

The buttons act only on the connection you selected, and only when you press them — and they work on outside (public) connections. Pick a row inside your own home network and the pane will tell you: “Pick an outside connection first.” Nothing is ever sent out about your own private addresses.

What each answer means, in one line

- VirusTotal: “N engines say malicious · N suspicious · N harmless” — the scanners' vote, counted in the open.
- AbuseIPDB: “Abuse confidence N/100 · N reports” — how strongly the reporting crowd believes this address misbehaves. No button: with a key saved, this check runs by itself and its line appears with the others.
- GreyNoise: whether the address is “seen scanning the internet,” what it is classed as, and whether it sits in the known-benign services set — background noise vs. something with your name on it.
- URLhaus: quiet when there's nothing to say; a ▲ warning line — “This host has served malware links” — when there is.

Above those lines, the pane gives the verdict — the worst honest reading of everything the checks said: KNOWN BAD, SUSPICIOUS, KNOWN SAFE, or NO BAD REPORTS (which the app is careful to say is not a promise it's safe) — followed by a WHAT SHOULD I DO? section in plain words.

No key yet? The buttons tell you the truth instead of failing quietly. Press Check with VirusTotal with no key saved and the pane answers: “VirusTotal is OFF — add your own free key in Settings to turn it on.” URLhaus answers the same way: “URLhaus needs your free abuse.ch key — add it in Settings.” GreyNoise asks for nothing — it just runs.

8 – KEY SAFETY + WHEN SOMETHING LOOKS WRONG

- A key leaked? Go back to that service, make a fresh key, and delete the old one — every service in this guide lets you do both — then paste the new key into OSINT (§6). The old key dies at the service, so a leaked copy is worthless.
- “Free allowance used up” (GreyNoise): not an error. The free day's checks are spent; the button works again tomorrow, and everything else keeps working tonight.
- A check says “failed”: the service didn't answer — the pane shows the address as unknown to that check, never as cleared. Try again later; an honest “no answer” is the design, not a bug.
- Being asked for a card, anywhere: stop. Every key in this guide is free. A card request means a paid plan got picked by mistake — back out and choose the free one named in the steps.
- Lost the key you made? Sign back into the service — VirusTotal and abuse.ch show your key on your profile/API page; on AbuseIPDB, press Show beside the key you created. Then §6 again.

That's the whole of it. Four free keys, each fetched from its own service, pasted once into Settings, working from your own computer — and an app that tells you plainly what it sends, what it found, and what it doesn't know. Check who your machine is talking to. That's what OSINT is for.

OSINT — Live Connections Viewer · 777 Software. This guide ships with the app. The services named here are run by their own people; their sign-up pages may rearrange their furniture over time, but the shape — free account, verify your email, find the key on your profile — does not change.