How Online Scams Really Work: What OSINT Can Reveal Before You Lose Money

Maria Cattini | 03/12/2025 | CYBERSECURITY

Ever wondered how thousands of people can fall for the *same* online investment scam, even when the warning signs are obvious in hindsight?
The truth is uncomfortable: modern scams look professional, speak your language, mimic real companies and hide inside networks that span continents.

A recent cross-border investigation revealed how a suspected criminal group deceived **over 70,000 victims** across Europe and beyond, running fake trading platforms from call centres disguised as tech firms. The network allegedly earned **250 million euro**, using pressure, theatrics and cloned websites to drain bank accounts.

If this happened to so many people, the question becomes simple: *how do you protect yourself?*
This is where **OSINT** becomes a practical ally.

Why Online Scams Are Getting So Sophisticate

Scammers abandoned the messy spelling errors and broken websites of the past. Today they run operations that look cleaner than many legitimate businesses.

Fake companies look real

The case documented in the investigation showed offices in Belgrade set up like any modern start-up: open space, good lighting, branded desks, multilingual staff and scripts ready for every objection.

Nothing screamed “criminal operation”.

Social engineering is industrial-scale

Victims described daily phone calls from “brokers”, apparently fluent in their language and trained to keep conversations friendly, persuasive and urgent.
One Belgian victim reported his account balance rising to 3,000 euro before access suddenly vanished.

Even big brands get entangled

One scam brand became a **partner of Leeds United**, gaining visibility across Premier League broadcasts before authorities revoked its licence for misleading promotions.

When a scam rides inside a football sponsorship, you realise the scale.

What OSINT Can Uncover in Minute

You don’t need to be a technician. You need curiosity, patience, and a few checks that anyone can

run.

1. The company address test

Search the company’s address on Google Maps.
In the case of “Greenfields Capital”, one victim noticed the London address didn’t actually exist.
A missing office is usually enough to walk away.

2. Registry and licence checks

Most financial services need a licence.
Before trusting a trading platform:

• look it up on the financial authority’s register (FCA, BaFin, CONSOB, etc.)
• check if the licence was revoked
• scan warnings on regulators’ websites

The investigation revealed revoked licences, lawsuits and regulatory bans buried in public records that victims never checked.

3. WHOIS, domain age and hosting location

A trading platform registered only a few months ago, hosted in a tax haven, should trigger suspicion fast.
You can check it with tools such as:

• whois.domaintools.com
• hostingchecker
• urlscan.io

Most scam platforms in the investigation had **short-lived domains** tied to shell companies.

4. Reverse-image lookup

Take the “broker’s” photo from their email signature or website and run it through:

• Google Lens
• Yandex Images
• PimEyes

Scam call centres often used **AI-generated portraits** or faces stolen from random social profiles.
If you find the same face on several unrelated sites, run.

5. Tracking the money path

Scam deposits often pass through cryptocurrency gateways or payment processors registered in countries with minimal oversight.
In the revealed scheme, deposits were routed through platforms linked to offshore structures in Estonia and Australia.

If your “broker” asks for crypto transfers, the conversation should end there.

A Simple OSINT Workflow You Can Use Before Clicking “Invest”

A practical routine you can follow in less than 10 minutes.

Step 1: Check the domain

• Age
• Registrar
• Country of hostingAnything under one year should worry you.

Step 2: Run the address and phone search

Paste the contact address into Maps.
Paste the phone number into Google with quotes.
If nothing comes up, avoid it.

Step 3: Verify the human behind the email

Run their name and picture through search engines.
Legitimate professionals leave traces: conference panels, LinkedIn profiles, publications.

Step 4: Scan for past complaints

Search the brand + “scam”, “review”, “warning”, “forum”.
Don’t stop at page one of Google.

Step 5: Check regulators

FCA, CONSOB, ASIC, CySEC, BaFin publish warnings daily.
Two minutes here can save your savings.

Why OSINT Works So Well for Ordinary People

OSINT is not hacking.
It is simply the habit of checking *before* trusting.

The leaked chats from the Belgrade call centres showed employees calling victims “idiots” for believing the fake profits displayed on manipulated dashboards.

OSINT turns the tables.
You no longer behave like an easy target.
You become the person they cannot fool.

Tools for Everyday OSINT (Non-Technical and Safe)

Below are tools you can use without any cybersecurity skills:

1. Wayback Machine

See past versions of a website.
If a trading site has “born yesterday” pages, that’s revealing.

2. Whoisology / ICANN Lookup

Check domain ownership patterns.

3. Company registry portals

• UK Companies House
• Italian Registro Imprese
• EU Business Registers

These expose shell companies faster than any phone call.

4. URLScan.io

Shows what external servers a website contacts.
Scam sites often ping suspicious servers.

5. Reverse image tools

To confirm that profile photos actually belong to a real human.

Risks and Limits

No single method protects you completely.
But each OSINT check increases your safety.

Pros

• Fast and free
• Works on any suspicious platform
• Reduces emotional decision-making
• Adapts to any type of scam (investments, romance, job offers)

Cons

• Scammers constantly rebrand
• Some results require interpretation
• False positives may occur with new legitimate companies

Still, when the alternative is losing a lifetime of savings, OSINT becomes common sense.

The massive scam uncovered across Europe proves one thing: **anyone** can be fooled when the fraud looks professional and friendly.
You don't need technical expertise. You need habits.

Before signing up, sending money or trusting a "broker", run five minutes of OSINT.
It may save you months of regret.

If you want to sharpen your OSINT skills with practical, non-technical guides, join the Project OSINT community.

Subscribe: https://projectosint.substack.com/
Telegram group: https://t.me/osintprojectgroup

Stay sharp. Stay informed. Stay impossible to scam.

Ever wondered how thousands of people can fall for the *same* online investment scam, even when the warning signs are obvious in hindsight?
The truth is uncomfortable: modern scams look professional, speak your language, mimic real companies and hide inside networks that span continents.

A recent cross-border investigation revealed how a suspected criminal group deceived **over 70,000 victims** across Europe and beyond, running fake trading platforms from call centres disguised as

tech firms. The network allegedly earned **250 million euro**, using pressure, theatrics and cloned websites to drain bank accounts.

If this happened to so many people, the question becomes simple: *how do you protect yourself?* This is where **OSINT** becomes a practical ally.

Why Online Scams Are Getting So Sophisticate

Scammers abandoned the messy spelling errors and broken websites of the past. Today they run operations that look cleaner than many legitimate businesses.

Fake companies look real

The case documented in the investigation showed offices in Belgrade set up like any modern start-up: open space, good lighting, branded desks, multilingual staff and scripts ready for every objection.

Nothing screamed “criminal operation”.

Social engineering is industrial-scale

Victims described daily phone calls from “brokers”, apparently fluent in their language and trained to keep conversations friendly, persuasive and urgent.
One Belgian victim reported his account balance rising to 3,000 euro before access suddenly vanished.

Even big brands get entangled

One scam brand became a **partner of Leeds United**, gaining visibility across Premier League broadcasts before authorities revoked its licence for misleading promotions.

When a scam rides inside a football sponsorship, you realise the scale.

What OSINT Can Uncover in Minute

You don’t need to be a technician. You need curiosity, patience, and a few checks that anyone can run.

1. The company address test

Search the company’s address on Google Maps.
In the case of “Greenfields Capital”, one victim noticed the London address didn’t actually exist.
A missing office is usually enough to walk away.

2. Registry and licence checks

Most financial services need a licence.
Before trusting a trading platform:

- look it up on the financial authority’s register (FCA, BaFin, CONSOB, etc.)
- check if the licence was revoked
- scan warnings on regulators’ websites

The investigation revealed revoked licences, lawsuits and regulatory bans buried in public records that victims never checked.

3. WHOIS, domain age and hosting location

A trading platform registered only a few months ago, hosted in a tax haven, should trigger suspicion fast.
You can check it with tools such as:

• whois.domaintools.com
• hostingchecker
• urlscan.io

Most scam platforms in the investigation had **short-lived domains** tied to shell companies.

4. Reverse-image lookup

Take the “broker’s” photo from their email signature or website and run it through:

• Google Lens
• Yandex Images
• PimEyes

Scam call centres often used **AI-generated portraits** or faces stolen from random social profiles.
If you find the same face on several unrelated sites, run.

5. Tracking the money path

Scam deposits often pass through cryptocurrency gateways or payment processors registered in countries with minimal oversight.
In the revealed scheme, deposits were routed through platforms linked to offshore structures in Estonia and Australia.

If your “broker” asks for crypto transfers, the conversation should end there.

A Simple OSINT Workflow You Can Use Before Clicking “Invest”

A practical routine you can follow in less than 10 minutes.

Step 1: Check the domain

• Age
• Registrar
• Country of hostingAnything under one year should worry you.

Step 2: Run the address and phone search

Paste the contact address into Maps.
Paste the phone number into Google with quotes.
If nothing comes up, avoid it.

Step 3: Verify the human behind the email

Run their name and picture through search engines.
Legitimate professionals leave traces: conference panels, LinkedIn profiles, publications.

Step 4: Scan for past complaints

Search the brand + “scam”, “review”, “warning”, “forum”.
Don’t stop at page one of Google.

Step 5: Check regulators

FCA, CONSOB, ASIC, CySEC, BaFin publish warnings daily.
Two minutes here can save your savings.

Why OSINT Works So Well for Ordinary People

OSINT is not hacking.
It is simply the habit of checking *before* trusting.

The leaked chats from the Belgrade call centres showed employees calling victims “idiots” for believing the fake profits displayed on manipulated dashboards.

OSINT turns the tables.
You no longer behave like an easy target.
You become the person they cannot fool.

Tools for Everyday OSINT (Non-Technical and Safe)

Below are tools you can use without any cybersecurity skills:

1. Wayback Machine

See past versions of a website.
If a trading site has “born yesterday” pages, that’s revealing.

2. Whoisology / ICANN Lookup

Check domain ownership patterns.

3. Company registry portals

• UK Companies House
• Italian Registro Imprese
• EU Business Registers

These expose shell companies faster than any phone call.

4. URLScan.io

Shows what external servers a website contacts.
Scam sites often ping suspicious servers.

5. Reverse image tools

To confirm that profile photos actually belong to a real human.

Risks and Limits

No single method protects you completely.
But each OSINT check increases your safety.

Pros

• Fast and free
• Works on any suspicious platform
• Reduces emotional decision-making

• Adapts to any type of scam (investments, romance, job offers)

Cons

• Scammers constantly rebrand
• Some results require interpretation
• False positives may occur with new legitimate companies

Still, when the alternative is losing a lifetime of savings, OSINT becomes common sense.

The massive scam uncovered across Europe proves one thing: **anyone** can be fooled when the fraud looks professional and friendly.
You don’t need technical expertise. You need habits.

Before signing up, sending money or trusting a “broker”, run five minutes of OSINT.
It may save you months of regret.

If you want to sharpen your OSINT skills with practical, non-technical guides, join the Project OSINT community.

Subscribe: https://projectosint.substack.com/
Telegram group: https://t.me/osintprojectgroup

Stay sharp. Stay informed. Stay impossible to scam.