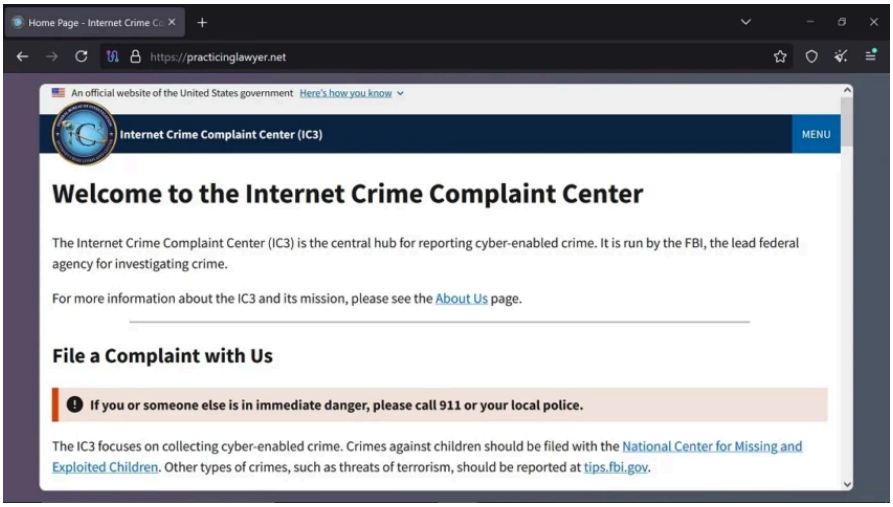
# FBI warns of threat actors spoofing the FBI crime complaint website

⋮ 9/26/2025


The FBI has issued an alert warning users that its Internet Crime Complaint Center (IC3) site is being spoofed. IC3 is the go-to centralized site where the FBI receives all cybersecurity complaints. Fake IC3 sites not only lure victims into giving away sensitive data and funds but also erode the trust of the general public, who are already cautious about reporting cybercrimes.

## Fake IC3 sites are luring in victims seeking to report crimes to the FBI

On September 19, the FBI warned that threat actors were spoofing the FBI's IC3 government website. This is not the first time this has happened.




This screenshot shows a fake IC3 FBI site. The entire HTML and site content seem to have been copied and pasted. However, if you che notice that it's fake. Image: Screenshot, Moonlock.

A similar warning was issued by the FBI on April 18.

The trend and technique of impersonating the FBI and IC3 go way back. Malwarebytes reported that between December 2023 and February 2025, the FBI received over 100 reports of scams involving people posing as IC3

employees.

Stay on top of cyber threats

Get cybersecurity news and lifehacks in our quick-to-the-point newsletter

Done!

Sorry, this email doesn't look right. Could you double-check it?

We've sent you a confirmation email, please take a look.

Thanks for subscribing!

We've sent you a confirmation email, please take a look.

The motive driving these FBI impersonation scams seems to be solely monetary and not nation-state driven. The scams are being spread through social media, social media messaging, malvertising, and search engine optimization (SEO) and/or sponsored results.

The use of these types of distribution channels — which casts a wide net, as opposed to more highly targeted spear phishing — is a clear indication that these are classic, financially driven scams and not sophisticated cyberattacks.

On Reddit, several users complained about having encountered fake FBI IC3 ads on platforms like Facebook, being contacted via social media messages, and even receiving phone calls.

A user on Reddit claimed 3 months ago to have encountered fake FBI ads on Facebook. Image: Screenshot, Moonlock.

While the FBI did not release a list of indicators of compromise (IoCs), these being the website URLs hosting the fake IC3 site, BleepingComputer found the following domains linked to this specific campaign:

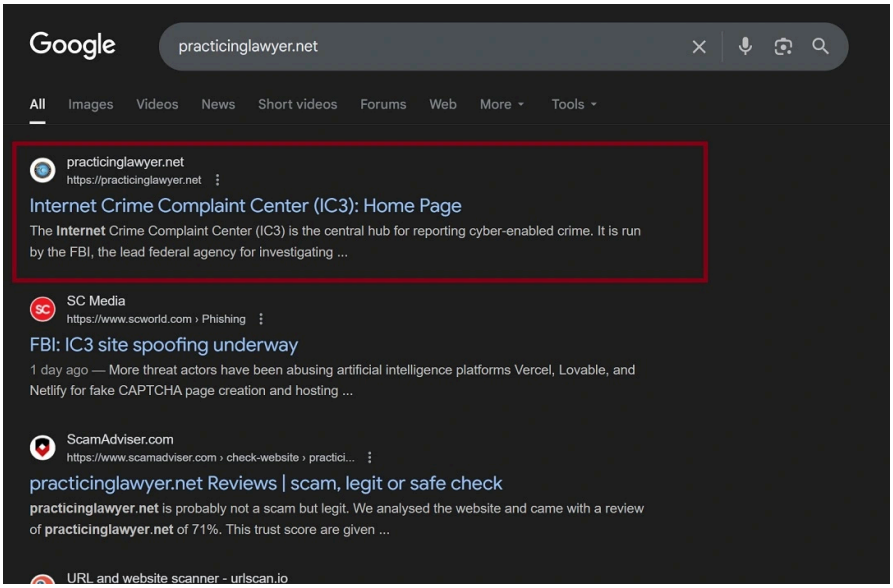
- cc3[.]live (defunct)
- practicinglawyer[.]net (still active)
- Ic3a[.]com (defunct)

It seems safe to assume there are at least a couple more of these fake IC3 sites online.

### A closer look at a website impersonating the FBI's IC3 (Internet Crime Complaint Center)

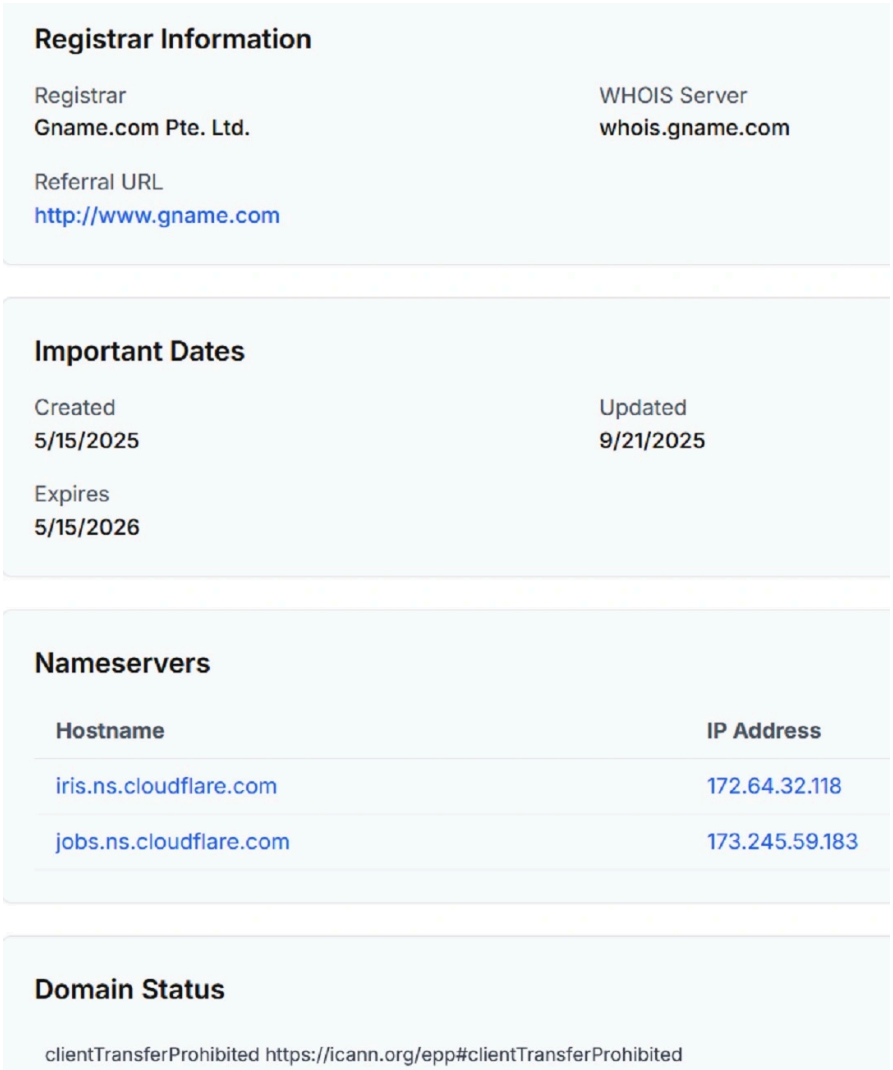
At the time of this writing, the only active site was practicinglawyer[.]net. Threat actors who built this site seemed to have simply copied and pasted most of the original content or HTML from the original FBI site onto a new domain. Even the FBI's contact phone numbers on the fake site are identical to the legitimate IC3 site.

The site itself does not appear to host any malicious scripts or dangerous cookies. However, the site did rank in the number-one position on Google search when specific keywords were used, as shown in the image below.



This screenshot shows a fake IC3 site listing, active in Google Search (top of the page). Image: Screenshot, Moonlock. Google Search is LLC.

This high ranking in Google Search tells us that the threat actors are SEO capable and have decent website-building skills.



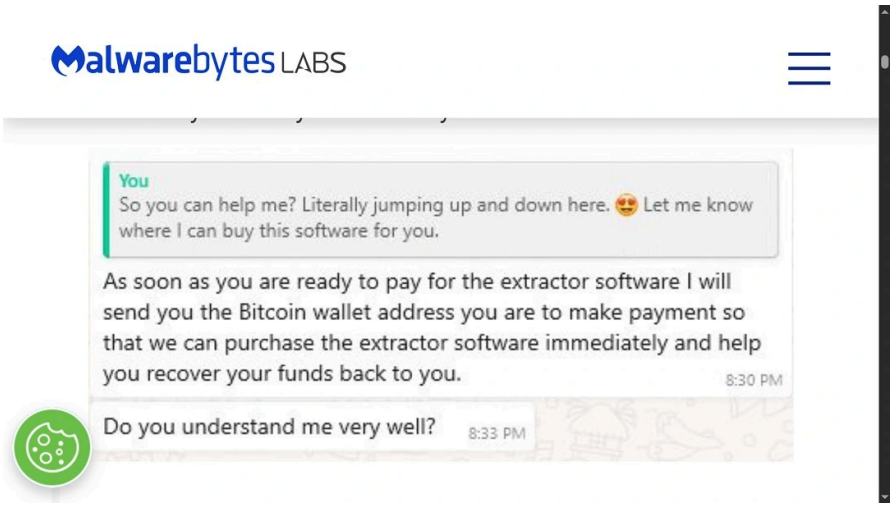
WHOIS data shows that the fake IC3 site was created 3 months ago, in May 2025. Image: Screenshot, Moonlock.

## How does the fake FBI IC3 scam work?

Impersonating the FBI is a high-risk tactic that threat actors use in hopes of luring high-value victims. However, tricking users into paying for FBI services is a clear red flag that anyone would spot. So, how do scammers do it? How do they convince victims to pay a federal agent?

Malwarebytes' recent investigation into an FBI spoofing scam has the answer to that question.

The threat actors posing as FBI agents or IC3 workers tell victims that they can recover stolen funds (usually crypto) and ask victims to pay for the "recovery software" or "extractor software."

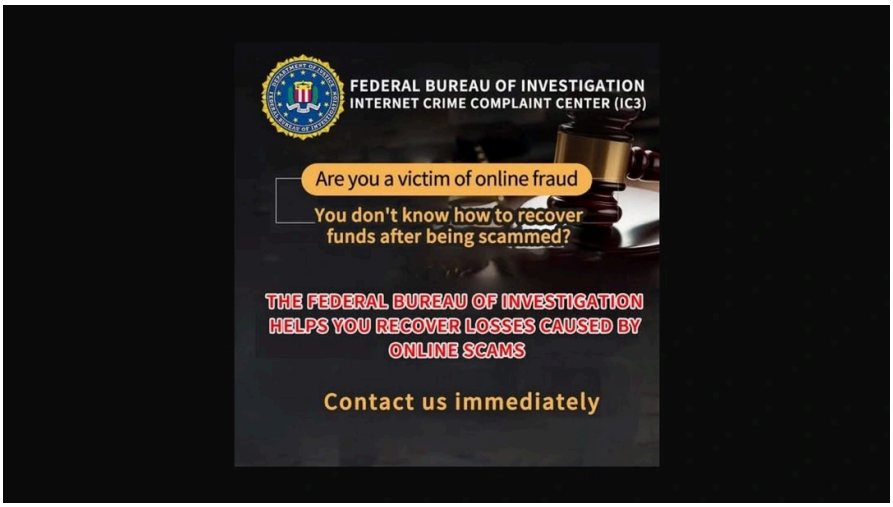


Malwarebytes shared a screenshot of how scammers trick users into paying for the FBI to recover stolen funds. Image: Screenshot, Moo

This is most likely just one of the ways in which these attackers work to trick victims who report cybercrimes to fake IC3 sites.

Overall, the fake FBI scam works as follows:

1. Victims of a cybercrime look for the IC3 site to file a crime complaint.
2. Victims reach a fake IC3 site, either through search engine results or social media, and contact the threat actors who are spoofing the FBI.
3. A fake FBI agent or fake IC3 worker follows up via phone, email, or social media messaging.
4. The victims are asked for sensitive information and eventually tricked into paying to recover funds, which, of course, are never recovered.



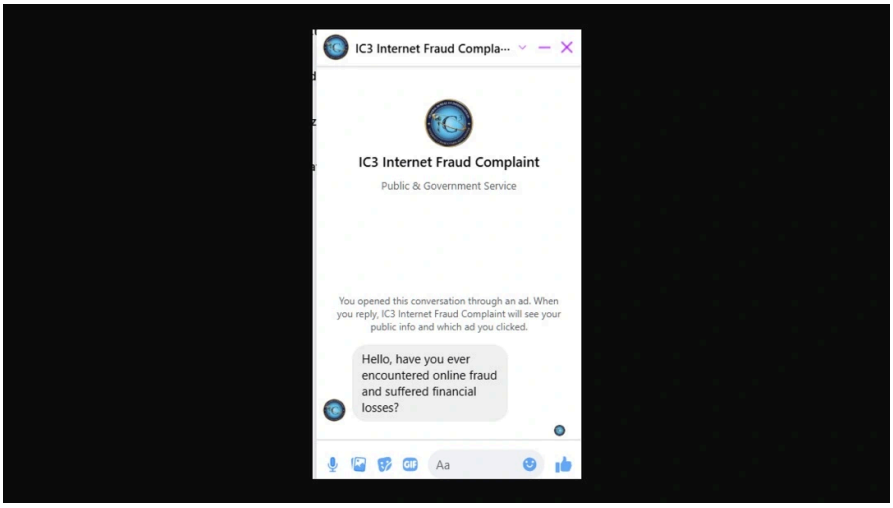
A user on Reddit shared what he said was a fake FBI ad on Facebook. Image: Screenshot, Moonlock.

## How to stay safe and avoid the fake FBI scam

Hoping to help users stay safe, the FBI issued the following recommendations:

- **Do not pay for FBI services:** The IC3 and FBI will never ask for payment to recover lost funds or refer you to a company that charges for recovery.
- **Keep your personal data private:** Never share sensitive information with people you only know online or over the phone.
- **Know how the FBI contacts you:** The IC3 will not reach out through phone, email, social media, apps, or public forums. If more details are needed, you'll hear directly from an FBI field office or law enforcement officer.
- **Watch for recycled scams:** Scammers may change names and tactics, but the schemes typically stay the same.
- **Don't send money to strangers:** Avoid sending cash, gift cards, cryptocurrency, or other assets to people you haven't met in person.

It is also important to never underestimate the social engineering skills of scammers. You might think these types of scams are something you would never fall for, but in reality, when you are being scammed, you don't realize it until it's too late.



This screenshot allegedly shows a scammer impersonating an IC3 worker contacting a victim via social media messaging. Image: Screer

Bottom line: Never underestimate scammers' skills. Scammers are bold and are willing to go so far as to impersonate federal agents without thinking about the consequences. Many use professional-looking websites, fake caller IDs, or convincing stories to appear legitimate.

## Final thoughts

Finally, it's important to stress that even with these spoofing campaigns, individuals and companies alike who are affected by cybercrime should report incidents directly through the official IC3 website. Filing a report helps law enforcement provide the right support to victims and strengthens the overall cybersecurity community.

Ray Fernandez

Ray has been covering tech and cybersecurity for over 15 years. His work has appeared on TechRepublic, VentureBeat, Forbes, Entrepreneur, and the Microsoft Blog, among others.