The Fake Bureau of Investigation: How Cybercriminals Are Impersonating Government Pages

Shawn Hays ⋮ ⋮ 9/29/2025

Blog Threat Research

The FBI is noticing a large uptick in fraudulent websites impersonating the IC3. Learn how users are unsuspectingly reporting cybercrime to cybercriminals.

 Shawn Hays

4 min read

Last updated September 29, 2025

Bad actors using AI and vibe coding tools to generate phishing sites at machine speed are making it harder for users to distinguish between legitimate and malicious content.

To help security teams, we're diving into the latest tactics attackers are using, recent attempts to clone the FBI IC3 site, and why traditional security measures may no longer be enough to defend against evolving threats.

What is the IC3, and how are cybercriminals impersonating it?

In the FBI's latest notice (September 2025), they describe a large uptick in fraudulent websites popping up and impersonating the Internet Crime Complaint Center (IC3). IC3 traditionally serves as a trusted location for individuals to report cybercrime. However, you may now be accidentally reporting cybercrime to cybercriminals.

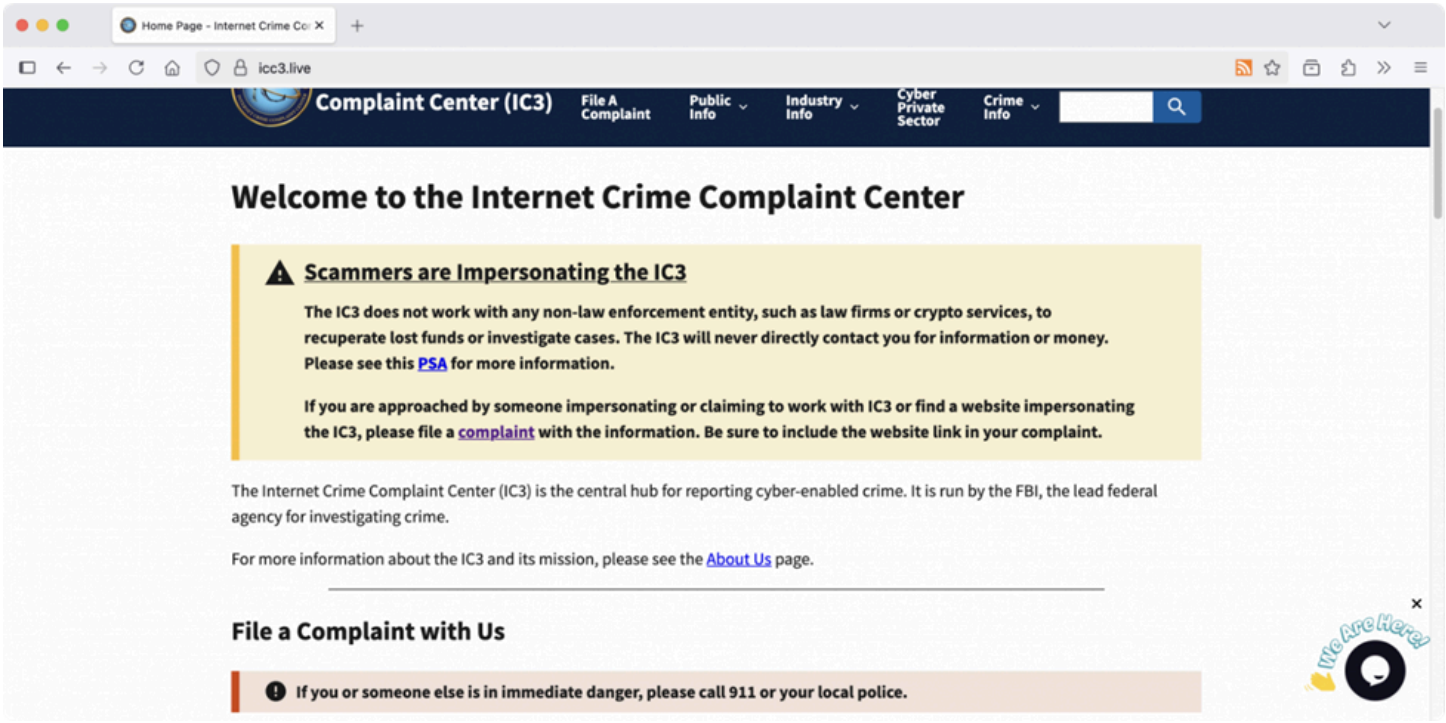
According to research by BleepingComputer, several examples of websites staged as fake FBI reporting sites included "icc3[.]live", "practicinglawyer[.]net", and "ic3a[.]com". Varonis also found dozens of examples that are now presumably taken down by authorities or attack groups. Here's a list of 30 for reference:

ic3-gov.com	ic3-reporting.org	icc3.net
ic3gov.org	fbi-ic3.net	ic3a.org
malicious-ic3.net	ic3crimecenter.com	ic3-reporting.net
icc3.live	reportic3.org	fbi-ic3.org
ic3a.com	ic3complaint.net	ic3crimecenter.org
ic3-report.net	ic3security.org	reportic3.net
ic3help.org	ic3-fbi.org	ic3complaint.org
fbi-ic3.com	ic3helpdesk.com	ic3security.live
ic3support.net	ic3online.net	ic3-fbi.com
report-ic3.org	ic3form.org	ic3helpdesk.org

The IC3 started in 2000, and according to then IC3 Chief Donna Gregory at the 20th anniversary, "people really didn't know where to report internet scams or other online fraudulent activity, and law enforcement agencies were saying: 'What do we do with these? How do we handle them?'" Ironically, bad actors are betting that users still don't where to report in 2025.

Attackers are establishing domains with similar or familiar elements like 'FBI', 'IC3', and 'report/ing' in hopes of luring some unsuspecting guests to populate reporting forms with personally identifiable information (PII), technical or networking details, and other forms of organizational data. Worse, the sites are often near-exact replicas of IC3's site, including warning notices about 'Scammers are impersonating the IC3'.

IC3 website spoofed by scammers (Source: Bleeping Computer)



IC3 website spoofed by scammers (Source: Bleeping Computer)

Fake Bureau of Investigation

The (real) FBI lists phishing and spoofing as the highest-reported crime types in their 2024 IC3 Annual Report. Therefore, it's no wonder that cybercriminals would eventually attempt to imitate the IC3's website for phishing purposes.

Tens of thousands of new spear-phishing sites go online each day. Some of them closely resemble their target inspiration, such as the FBI IC3 example. Many others are hosted on legitimate infrastructure like adobe[.]com, canva[.]com, dropbox[.]com, onedrive[.]live.com app[.]box[.]com, and alchemy[.]com. to name a few.

Secure web gateways, URL filtering, legacy malware protection, browser isolation, and internet policies are all strategies to defend users from web threats. However, these strategies are struggling to keep pace with fast-moving web-based phishing threats, leaving corporations exposed to all manner of exploitation.

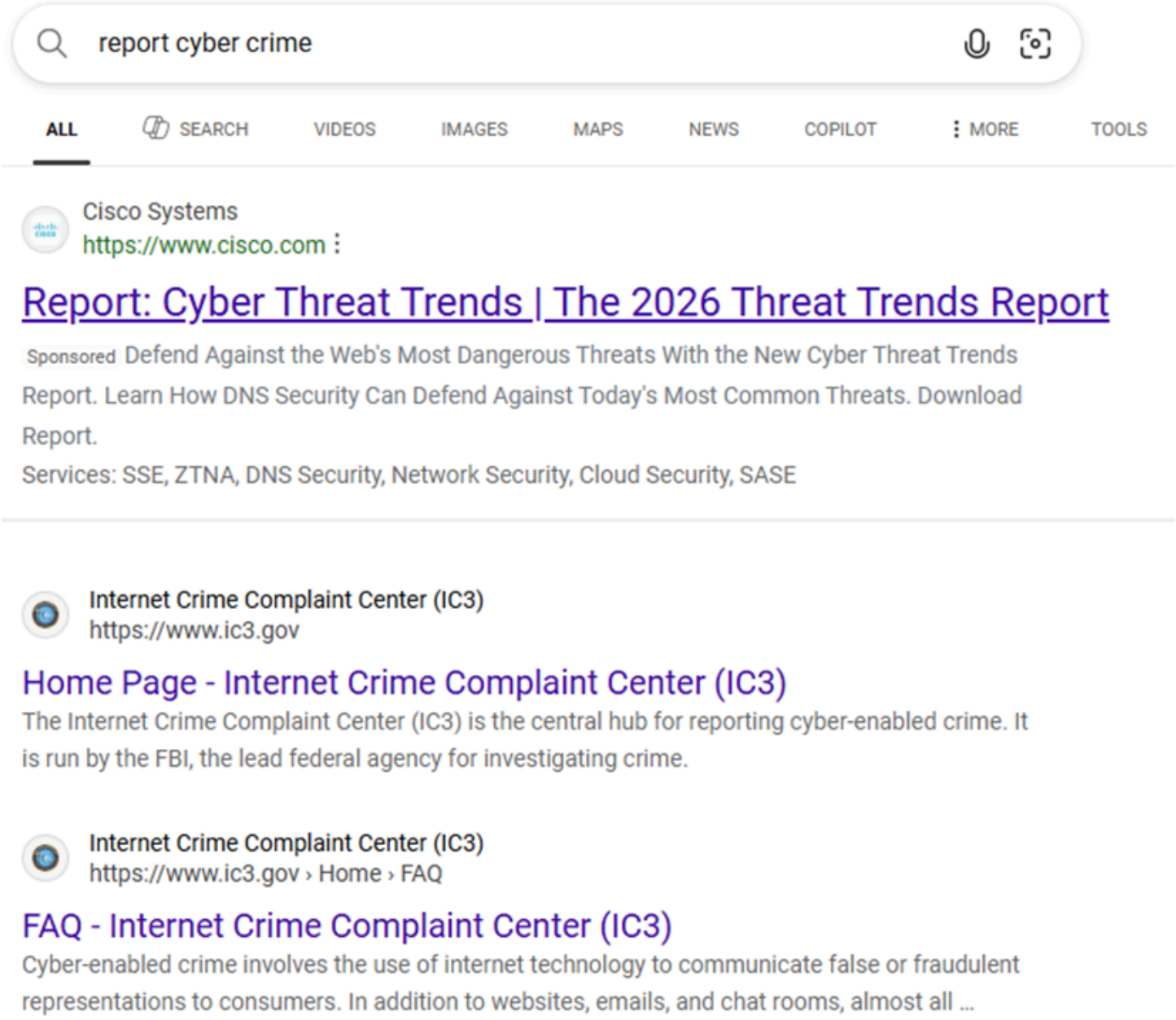
Long gone are the days when poor spelling, badly pixelated company logos, and unbelievable claims from overseas asking for access to bank accounts made phishing attempts easy to spot. Today's cybercriminals are using much more sophisticated approaches that humans need intelligence and machines to help identify the fraud.

SEO Poisoning and Malvertising

Have you ever clicked on the first link in search results, even if you see the often subtle 'Sponsored' indicator? If you haven't, your users likely have.

A quick experiment with “report cybercrime” shows a sponsored resource that appears to be safe. Yet users don’t often check for signs of impersonated sites, nor can they spot a possibly malicious site when the attackers use the FBI logo as the favicon (icon image left of the search result).

Example of a sponsored link placement that cybercriminals can exploit



Example of a sponsored link placement that cybercriminals can exploit

SEO poisoning or SEO phishing is a relatively inexpensive way for bad actors to prey on users’ expeditious tendencies to trust and select the first result they see in a search. Malvertising is another term for this tactic, where attack groups use the same engines marketers leverage to purchase paid search ad space.

Sometimes the best cybercriminals are also the best marketers.

True multimodal AI for email and browser Security

Phishing websites and spoofing have become a leading cybersecurity challenge for organizations. Users need browsers to access SaaS applications and conduct a large portion of their daily work, but there's no level of training and awareness that can prepare them for modern impersonation tactics.

The answer is to apply multiple layers of artificial intelligence (AI) and machine learning (ML) to every aspect of the attack chain.

1. **Domain and link analysis**: Lean on a robust threat intelligence database and feed, along with WHOIS domain monitoring for all newly registered domains.
2. **Computer vision**: Rely on uniquely tuned visual scanning to analyze every aspect and pixel of a website — including webpage logo, layout, and other visual elements for deviations.
3. **Phishing Sandbox**: See through obfuscation techniques like Cloudflare's Turnstile Services and CAPTCHA validation gates by enabling AI and machines to emulate the full user journey and inspect every redirect or destination. This is critical for sites that have not been registered in any threat feed and are newly generated.

Your organization also needs advanced browser security with a trustworthy extension to block sites flagged by the outlined AI solutions above. By harnessing AI and ML, we can secure browsers and preemptively stop attacks that target users, such as employees or citizens looking to report cybercrime to the FBI IC3.

Additional recommendations

When it comes to the IC3, the FBI also recommends following these precautions:

- Type www.ic3.gov directly into the address bar located at the top of your Internet browser, rather than using a search engine
- If using a search engine, avoid any "sponsored" results as these are usually paid imitators looking to deter traffic from the legitimate IC3 website
- Verify that the URL of the IC3 website ends in [.]gov
- Avoid clicking on any link whose URL differs from the legitimate IC3
- Never click on links that may include suspicious artifacts or graphics, such as unprofessional or low-quality graphics used to imitate a legitimate website

While the FBI's recommendations are crucial for direct user training, they may not be sufficient to thwart advanced attacks. Cybercriminals are constantly evolving their tactics, making it increasingly difficult for users to identify anomalous graphics or websites. These sophisticated attacks often mimic legitimate sources so convincingly that even vigilant users can be deceived.

It is essential to complement the FBI's guidelines with advanced browser security measures and continuous AI-powered analysis to stay ahead of these threats.

What should I do now?

Below are three ways you can continue your journey to reduce data risk at your company:

1

Schedule a demo with us to see Varonis in action. We'll personalize the session to your org's data security needs and answer any questions.

2

See a sample of our Data Risk Assessment and learn the risks that could be lingering in your environment. Varonis' DRA is completely free and offers a clear path to automated remediation.

×

Shawn Hays Shawn is a Product Marketing Manager for Varonis, focusing largely on AI and the Microsoft cloud. He has been a journeyman in the Microsoft ecosystem and cybersecurity arena for ten years. When not pontificating on AI and data security, you can catch him at a music festival or throwing a frisbee.