# U.S. Justice Department will no longer bring charges against good-willed security researchers

BY ANNA HAMMOND · JUNE 14, 2022 · LAST UPDATED ON MARCH 6, 2025

There was big news for the crowdsourced ethical hacking community on May 19th this year. The U.S. Department of Justice revised its policy in respect to "ethical" or "good-faith" hackers. It will no longer prosecute them under the Computer Fraud and Abuse Act (CFAA).

This is a welcome step forward in the recognition of the important work done by ethical hackers. It will also benefit cybersecurity as a whole based within the jurisdiction of U.S Courts.

## Wait! Aren't "hackers" bad guys?

There's a lot of confusion around the term "hacker". Until May 19th, it seems even the U.S. Department of Justice was misusing the term.

"Hacker" in its broadest sense means "an individual who uses computer, networking or other skills to overcome a technical problem." But a combination of popular culture and growing awareness of cyber threats has led to the confusion of "hacker" with "malicious hacker"—those ill-intentioned players who work to breach the cybersecurity of software and systems.

At Intigriti, we're careful to call our security researchers "ethical hackers" to enforce the distinction between "ethical" and "malicious" security hackers working in the cybersecurity field. Now the U.S. Department of Justice is finally recognizing that distinction too.

## What's changing?

The global community of well intentioned hackers, working to help improve the cybersecurity for U.S. businesses and organizations, will now be able to breathe a collective sigh of relief.

Prior to this ruling, prosecutors could bring federal charges against ethical hackers working to find security flaws in vulnerable systems. It did not matter whether the hackers had good intentions and were working to *help* secure those systems.

The U.S. Department of Justice now wants to allow what it calls "good-faith security research" to be conducted without fear of prosecution, where the goal is "accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability." That sounds a lot like the work of crowdsourced bug bounty hunters!

## What this means for ethical hackers

The May ruling, put simply, means that cases will no longer be brought against ethical hackers that work to improve technology security. This should help to remove some of the stigma attached to the term

“hacker”. Far more importantly, it will clear the way for ethical hackers to work within the U.S. without legal threats arising from the nature of their work.

In our recent **Ethical Hackers Insights** survey, conducted with over 1,700+ security researchers, 96% said they would like to dedicate more time to working on bug bounty programs in the future.

Faced with increasing cyber attacks, many consider these programs the only way to anticipate the actions of malicious actors and patch up vulnerabilities *before* they are exploited.

At Intigriti, we provide a cutting-edge **bug bounty platform** that facilitates this important work done by over 50,000+ crowdsourced ethical hackers across the globe. We therefore welcome this change in U.S. Department of Justice policy that will allow our community to improve the security of businesses and organizations in the U.S. without fear of prosecution.

## Learn more

Intrigued by what you have read? Want to know more about bug bounty programs? Get in touch to **request a demo** with a member of our team today.

**REQUEST A DEMO**

**intigriti.com/demo**

**VISIT THE WEBSITE**

**intigriti.com**

**GET IN TOUCH**

**hello@intigriti.com**