



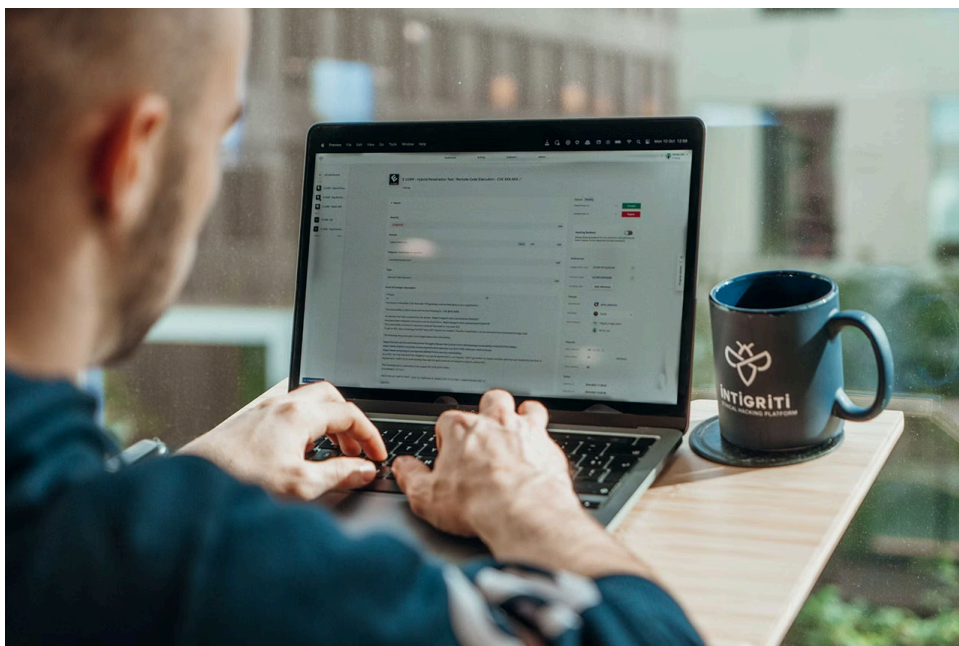
# The truth about ethical hackers: Are they trustworthy?

BY ANNA HAMMOND · APRIL 29, 2024 · LAST UPDATED ON MARCH 6, 2025

To outmanoeuvre cybercriminals, the key is to beat them to the punch by [working with ethical hackers](#). However, a question often arises: Can we trust ethical hackers? Especially when we don't know them personally?

Through platforms such as Intigriti, the short answer is **yes, you can trust these individuals**. However, the word 'hacker' carries a variety of meanings, many of which are negative. This can make companies hesitant to partner with security specialists of this kind. So, let's address these concerns. By the end of this article, you'll have a better understanding of why ethical hackers are not only trustworthy, but also essential partners in securing businesses today.

## What does an ethical hacker do?



Cybersecurity threats are constantly evolving—and [ethical hackers](#) are a vital resource in the fight against cyber threats. These skilled professionals use their knowledge to simulate real-world attacks, uncovering vulnerabilities that malicious actors could exploit.

The contributions of ethical hackers go beyond simply identifying vulnerabilities. They also play a critical role in empowering organizations to [improve their overall security posture](#). By conducting thorough assessments, ethical hackers can help organizations identify gaps in security policies, procedures, and technologies. This information can then be used to improve the organization's security defenses and minimize the risk of a successful cyberattack.

# Fostering trust and integrity in ethical hacking communities

Bug bounty platforms provide a structured and controlled environment where organizations can engage with a diverse community of skilled ethical hackers to identify and address vulnerabilities.

One way bug bounty platforms help foster trust is through rigorous vetting processes (we'll cover how Intigriti handles this below.) They also provide clear guidelines and rules of engagement for ethical hackers, ensuring that they understand the scope of the program and the expected behavior. Additionally, platforms facilitate effective communication channels between organizations and ethical hackers, allowing for prompt and efficient reporting of vulnerabilities and collaboration on their resolution.

Furthermore, bug bounty platforms offer financial incentives in the form of bounties for ethical hackers who successfully identify and report vulnerabilities.



These incentives not only attract skilled professionals to participate in bug bounty programs but also motivate them to invest their time and expertise in finding and responsibly disclosing vulnerabilities. By rewarding ethical hackers for their efforts, bug bounty platforms create a mutually beneficial relationship that encourages ongoing collaboration and trust.

## How Intigriti strikes the right balance between security and collaboration

To ensure the overall security and integrity of the platform, Intigriti meets [rigorous international security standards](#) and has established a security framework. For example, to participate in bug bounty programs, ethical hackers (also known as security researchers) must complete two steps:

1. **Researcher T&Cs:** Intigriti's legally binding [researcher T&Cs](#) include strict guidelines on confidentiality, data processing, non-disclosure of vulnerabilities, and more.

1. **ID Checks:** Intigriti's identity verification process involves thorough screening for potential fraud, stolen IDs, and impersonation.

Once accepted onto the platform, an [Intigriti Community Code of Conduct](#) becomes applicable for researchers, too. By implementing these measures, Intigriti ensures that trust and security are the top priorities of our bug bounty programs.

## Microsoft's experience with ethical hacking communities

Microsoft is just one of many organizations leveraging ethical hackers to strengthen their security posture. Microsoft runs a bug bounty program that pays out between \$13 to \$14 million per year to over 350 researchers, with rewards ranging from \$500 to \$250,000 per report. They have partnered with almost 10,000 researchers in total through Intigriti's platform.

Talking about their relationship with Intigriti's community, Madeline Eckert, Senior Program Manager on the Researcher Incentives team, says: "We look at the researcher community as our partners, not as our adversaries. They have a very different way of looking at our attack surface compared to those who are internal and potentially building the product itself. It's one of the key ways we can shore our surface from malicious actors."

## Do businesses need ethical hackers?

Ethical hackers are trusted partners for organizations seeking to protect their assets and maintain customer trust. Their expertise, professionalism, and commitment to ethical practices make them invaluable allies in the ongoing battle against cybercrime.

Bug bounty platforms also play a vital role in fostering trust and integrity within ethical hacking communities. They provide a secure and collaborative environment for organizations to engage with skilled ethical hackers, ensuring the identification and resolution of vulnerabilities.

Interested in inviting ethical hackers to contribute towards your security testing? Speak to a member of the Intigriti team today to [request a demo](#).

**REQUEST A DEMO**

[intigriti.com/demo](https://intigriti.com/demo)

**VISIT THE WEBSITE**

[intigriti.com](https://intigriti.com)

**GET IN TOUCH**

[hello@intigriti.com](mailto:hello@intigriti.com)