Hack The Government (HTG) 2025

Frequently asked questions

What is an “ethical hacker”?

Originally, the term *hacker* referred to people who were passionate about tinkering, capable of exploring and transforming all kinds of things (including ideas!). Over time, their field of activity has mainly shifted towards IT and technology. In essence, they are inventors who excel at discovery and innovation.

The concept of an “ethical hacker” is closely linked to IT security. It refers to “vulnerability hunters”, experts whose main mission is to track down flaws in IT systems. The key difference lies in their approach: constructive and resolutely legal.

Why is their work important in the field of cybersecurity?

The greatest dangers in an IT system lie in:

1. unaddressed (known) vulnerabilities;
2. unknown vulnerabilities (known as “zero-day” vulnerabilities).

It's all a question of time. In the first case, routine security audits or checks will identify and resolve the problem (in technical jargon, this is referred to as “patching” the vulnerability).

In the second case, the delay can be critical. Malicious actors can quickly exploit the flaw to attack or harm an organisation, with potentially devastating consequences, such as disruption to production or services.

What's more, with the rapid evolution of communication and information technology, the time it takes to exploit zero-day vulnerabilities is now generally less than 24 hours.

What is the role of the CCB?

The Centre for Cybersecurity Belgium (CCB) has a simple procedure to help people who discover security issues in software or IT services.

How does it work?

Anyone can report a security flaw, even if the organisation concerned does not have an official programme for this type of reporting. Here are some essential rules to follow.
For people who discover a vulnerability:

- You must act in good faith;
- You must not have malicious intentions;
- Limit your actions to what is strictly necessary to demonstrate the problem;
- Inform the organisation and the CCB directly.

Legal protection:

- If you follow these rules, you will be legally protected;
- Your actions will be considered constructive and responsible.

What is “Hack the Government”?

HackTheGovernment2025 is an initiative of the Centre for Cybersecurity Belgium (CCB) aimed at strengthening the digital security of Belgian public services.

Ethical hackers are invited to test the IT systems of certain public institutions, with the sole aim of detecting and reporting vulnerabilities in a responsible manner. More than just a competition, this is a genuine call for collaboration between all stakeholders, designed to raise the level of national cyber security.

Why is this important?

This process improves digital security in a collaborative and ethical manner. Rather than punishing individuals, it encourages them to actively contribute to collective protection.

Summary: this initiative mobilises benevolent experts to identify weaknesses in public IT systems, thereby anticipating potential attempts by malicious actors. It is a proactive approach that *ultimately* protects public services and, by extension, citizens.