

Hack The Government (HTG) 2025

Frequently asked questions

Qu'est-ce qu'un « hacker éthique »?

A l'origine, le terme *hacker* désignait des personnes passionnées de bricolage, capables d'explorer et de transformer toutes sortes de choses (y compris des idées !). Au fil du temps, leur domaine d'activité s'est principalement orienté vers l'informatique et la technologie. En substance, ils sont des inventeurs qui excellent dans la découverte et l'innovation.

La notion de « hacker éthique » est intimement liée à la sécurité informatique. Elle désigne des « chasseurs de vulnérabilités », des experts dont la mission principale consiste à traquer les failles dans les systèmes informatiques. La nuance essentielle réside dans leur démarche : constructive et résolument légale.

Pourquoi leur activité est-elle importante dans le domaine de la cybersécurité?

Les plus grands dangers dans un système informatique résident dans:

1. des vulnérabilités (connues) non prises en charge;
2. des vulnérabilités inconnues (dites "zero-day").

Tout est une question de temps. Dans le premier cas, des audits ou des contrôles de sécurité de routine permettront d'identifier et de résoudre le problème (dans le jargon, on parle de « patcher » la faille).

Dans le second cas, le délai peut s'avérer critique. Les acteurs malveillants ont alors la possibilité d'exploiter rapidement la faille pour attaquer ou nuire à une organisation, avec des conséquences potentiellement dévastatrices, comme l'interruption de la production ou des services.

Qui plus est, avec l'évolution rapide des techniques de communication et d'information, le délai d'exploitation des vulnérabilités "zero-day" se réduit désormais généralement à moins de 24 heures.

Quel est le rôle du CCB?

Le Centre pour la Cybersécurité Belgique (CCB) dispose d'une procédure simple pour aider les personnes qui découvrent des problèmes de sécurité dans des logiciels ou services informatiques.

Comment ça fonctionne ?

Tout le monde peut signaler une faille de sécurité, même si l'organisation concernée n'a pas de programme officiel pour ce type de signalement. Voici quelques règles essentielles à respecter.

Pour les personnes qui découvrent une faille :

- Vous devez agir de bonne foi ;
- Ne pas avoir d'intentions malveillantes ;
- Limiter vos actions au strict nécessaire pour démontrer le problème ;
- Informer directement l'organisation et le CCB.

Protection juridique :

- Si vous suivez ces règles, vous serez protégé·e légalement ;
- Votre démarche sera considérée comme constructive et responsable.

Qu'est-ce que « Hack the Government » ?

HackTheGovernment2025 est une initiative du Centre pour la Cybersécurité Belgique (CCB) visant à renforcer la sécurité numérique des services publics belges.

Les hackers éthiques sont invités à tester les systèmes informatiques de certaines institutions publiques, dans l'unique but de détecter et de signaler les vulnérabilités de manière responsable. Au-delà d'un simple concours, il s'agit d'un véritable appel à la collaboration entre tous les acteurs, destiné à élever le niveau de cybersécurité national.

Pourquoi est-ce important ?

Ce processus permet d'améliorer la sécurité numérique de façon collaborative et éthique. Plutôt que de sanctionner, on encourage les individus à contribuer activement à la protection collective.

Résumé: cette initiative mobilise les experts bienveillants pour identifier les faiblesses des systèmes informatiques publics, anticipant ainsi les tentatives potentielles des acteurs malveillants. C'est une approche proactive qui protège *in fine* les services publics et, par extension, les citoyens.