Government of the Netherlands

Fighting cybercrime in the Netherlands

The National Cyber Security Centre (NCSC) is responsible for overseeing digital security in the Netherlands. One of its main tasks is to make the Netherlands more resistant to internet crime. The NCSC falls under the authority of the National Coordinator for Counterterrorism and Security (NCTV).

› Responsible disclosure

Tasks of the NCSC

As the body responsible for digital security in the Netherlands, the NCSC carries out a number of tasks:

It continuously monitors all (potentially) suspect sources on the internet. When it identifies a threat (such as a virus or an attack on a website), it alerts public authorities and organisations.

It advises organisations on how to protect themselves from online threats.

It closely monitors developments in digital technology and updates security systems. This prevents such threats as the shutdown of telephone traffic.

Tips for using the internet safely

The NCSC gives tips to the public and organisations on counteracting cybercrime, and it runs information campaigns to highlight the risks. One of these campaigns is called 'Alert Online', which provides the public with ↗ useful tips on using the internet safely (in Dutch).

More powers for public authorities

The public authorities will be given more powers to fight cybercrime. A bill currently proceeding through parliament will authorise the police and prosecutors to:

arrest persons suspected of selling stolen digital data;

investigate or hack into suspects' computers remotely, for instance by installing software to detect serious forms of cybercrime;

intercept data or make it inaccessible, for instance by blocking child pornography or intercepting email messages containing information about offences.

These new powers will enhance police capability to fight crime on the internet - and deal with offenders

Have you discovered a security flaw in an ICT system belonging to central government? If so, contact the government body responsible, or email responsibledisclosure@rijksoverheid.nl. The flaw can then quickly be remedied. Notifying the government body concerned is called 'responsible disclosure'. If you do so, once the flaw has been remedied, you will be permitted to share information about it with the outside world.

See also

- Forms of cybercrime
- National Coordinator for Counterterrorism and Security (NCTV)

Ministry responsible

- Ministry of Justice and Security