



- Search
- [Register for alerts](#)
- [Register for alerts](#)

- [Home](#)
- [What we do](#)
- [Resources](#)
- [CiSP](#)
- [Contact us](#)

Navigation

- [Home](#)
- [What we do](#)

About us

CERT-UK is the UK National Computer Emergency Response Team, formed in March 2014 in response to the National Cyber Security Strategy. [The National Cyber Security Strategy](#), published in 2011, sets out the importance of strengthening the UK's response to cyber incidents.

CERT-UK has four main responsibilities that flow from the UK's Cyber Security Strategy:

1. National cyber-security incident management
2. Support to critical national infrastructure companies to handle cyber security incidents
3. Promoting cyber-security situational awareness across industry, academia, and the public sector
4. Providing the single international point of contact for co-ordination and collaboration between national CERTs

Co-ordination and collaboration

[CiSP »](#)

The Cyber-security Information Sharing Partnership (CiSP) is a joint industry/government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business. CiSP allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information.

[Who we work with »](#)

CERT-UK works closely with key partners to enhance the UK's ability to prepare for and manage national cyber-security incidents. This includes exercising with government departments and industry partners, sharing information with industry and academic computer emergency response teams and collaborating with national CERTs around the globe to enhance our understanding of the cyber threat.

Preventing cyber issues

[Best practice guides »](#)

CERT-UK, through the Cyber-security Information Sharing Partnership (CiSP), provides regular advice and guidance on a range of cyber issues, with the aims of sharing information and encouraging best practice amongst our partners.

[Other sources of advice »](#)

CERT-UK works primarily with other CERTs and companies that own and manage the critical national infrastructure (CNI). However, there are a number of other organisations that provide advice and support on cyber-security.

[News »](#)

Keep up to date on what's happening at CERT-UK and cyber-security more widely in the UK.

[Advisories »](#)

CERT-UK issues advisories that address cyber-security issues being detected across government, industry or academia, or, that offer best practice updates. This section contains all the latest advisories and the archives; you can also register to receive updates via the 'Register for alerts' page.

[Alerts »](#)

In the exceptional event of a critical national cyber-security incident, CERT-UK will issue an alert and appropriate guidance. You can find the latest alerts and the archives in this section, or you can register to receive updates via the 'Register for alerts' page.

[Register for alerts »](#)

You can follow our alerts published via Twitter, or subscribe to a range of RSS feeds covering some of our other publications.

Responding to a cyber issue

[Get help »](#)

CERT-UK works primarily with other CERTs and companies that own and manage the critical national infrastructure (CNI). However, there are a number of other organisations that can provide advice and support to help you to deal with a specific cyber incident.

You can...

- [Contact us](#)
- [Register for alerts](#)
- [Apply for CiSP membership](#)

Resources

- [Alerts](#)
- [Advisories](#)
- [Best practices](#)



[© Crown Copyright](#)

- [Terms of use](#)
- [Cookies](#)
- [Contact us](#)

Built by [Surevine](#)

All content is available under the [Open Government License v2.0](#), except where otherwise stated