Cyber Security: useful links

Data Protection

The publication "Protecting personal data in online services: learning from the mistakes of others", by the Information Commissioner's Office (ICO) discusses security issues that have frequently arisen during investigations of data security breaches by the ICO. These are: software updates; SQL injection; unnecessary services; decommissioning of software or services; password storage; configuration of SSL and TLS; inappropriate locations for processing data; and default credentials.

ICO - Protecting Personal Data in Online Services

Data Protection Self-Assessment Toolkit

Use the toolkit to assess your compliance with the Data Protection Act and find out what you need to do.

Information Sharing About Threats

Cybersecurity Information Sharing Partnership (CiSP)

The Cybersecurity Information Sharing Partnership (CiSP), part of CERT-UK[1], is a joint industry government initiative to share cyber threat and vulnerability information. CiSP allows members from across sectors and organisations to exchange cyber threat information in real time in a secure and confidential environment. CiSP members are also able to receive network monitoring reports. This free service allows users to receive tailored feeds of information from CERT-UK covering any malicious activity seen on your network.

IT Security

Information Commissioner's Office guidance – a practical guide to IT Security

Aimed at small businesses and gives advice on how to keep IT systems safe and secure.

Miscellaneous

Be Cyber Streetwise

The 'Be Cyber Streetwise' campaign is a cross-government campaign, funded by the National Cybersecurity Programme, and delivered jointly with the private and voluntary sectors. The campaign is led by the Home Office, working closely with the Department for Business, Innovation and Skills (BIS) and the Cabinet Office. They aim to measurably and significantly improve the online safety behaviour and confidence of consumers and small businesses (SMEs).

Ten Steps to Cybersecurity

Guidance for organisations looking to protect themselves in cyberspace.

[1] 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, updated in 2022 (published 2011), sets out the importance of strengthening the UK's response to cyber incidents.

Standards in Cybersecurity

Cyber Essentials Scheme

The Cyber Essentials scheme is a government-backed, industry supported scheme to help organisations protect themselves against common cyberattacks. The Cyber Essentials scheme provides businesses, small and large, with clarity on good basic cybersecurity practice. By focusing on basic cyber hygiene, your company will be better protected from the most common cyber threats. It enables organisations to gain one of two Cyber Essentials badges.

ISO/IEC 27001: Information Security Management

The Information Security Management system is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. Certification to ISO/IEC 27001 is possible but is not obligatory.

Training

Training in Cybersecurity for Legal and Accountancy professionals

Develop strategies to develop Cyber resilience – see website for details.