GOV.UK

Search

Home > UK Digital Strategy

Department
for Culture
Media & Sport

The internet has been an unquestionable force for economic and social progress. Its open and global character makes it an extraordinarily powerful tool for freedom, innovation, growth and knowledge. The increasing uptake of internet-based technologies worldwide has brought, or will bring, significant advantages to connected societies such as ours.

But as our reliance on technology grows, so do the opportunities for those who would seek to compromise our systems and data. Responding to this threat and ensuring the safety and security of cyberspace is an essential requirement for the entire digital economy. The benefits of digital will only continue if people and businesses feel safe and confident whilst online.

We therefore need to secure our technology, data and networks in order to keep our businesses, citizens and public services protected. We will continue to work with international partners to protect a free, open and secure internet that supports our economic prosperity and social well-being. And we must also do all we can to make sure that children and young people are protected from exposure to dangerous, inappropriate or harmful content online.

Cyber security

The new National Cyber Security Strategy published on 1 November 2016 sets our vision for the UK in 2021 as secure and resilient to cyber threats, prosperous and confident in the digital world. To realise this vision we will work to achieve the following objectives:

- Defend: we have the means to defend the UK against evolving cyber threats. We are equipped to respond effectively to incidents. UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves
- Deter: the UK will be a target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so
- Develop: we have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national requirements across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges

These objectives are underpinned by our actions across the world, including by investing in partnerships that shape the global evolution of cyberspace.

The key elements of the government’s strategy for achieving these objectives include:

- levers and incentives. We will support start-ups and invest in innovation. We will also explore all regulatory levers, including the forthcoming General Data Protection Regulation (GDPR), to drive improvements in cyber risk management across the economy
- expanded intelligence and law enforcement. The intelligence agencies, the Ministry of Defence, the police and the National Crime Agency, in coordination with international partner agencies, will expand their efforts to identify, anticipate and disrupt hostile cyber activities by foreign actors, cyber criminals and terrorists
- development and deployment of technology in partnership with industry, including Active Cyber Defence measures, to deepen our understanding of the threat, strengthen the security of the UK public and private sector systems and networks and disrupt malicious activity. These measures, once implemented, will automatically counter the most common forms of malicious activity in cyberspace – highly prolific, damaging but often low-sophistication cyber attacks
- National Cyber Security Centre (NCSC), a single new central body for cyber security at a national level. Its role is to manage national cyber security incidents, provide an authoritative voice and centre of expertise on cyber security, and deliver tailored support and advice to government departments, the devolved administrations, regulators and businesses. The NCSC will analyse, detect and understand cyber threats, and will also provide its cyber security expertise to support the government’s efforts to foster innovation, support a thriving cyber security industry and to develop cyber security skills

In the Strategic Defence and Security Review 2015, the government set aside £1.9 billion over the five years of the strategy to deliver on these commitments and objectives.

We will also provide the pipeline of cyber skills that the country needs to actively secure and defend against potential and established threats. These measures will underpin the digital skills agenda and ensure that the UK economy has the skills and capacity to protect businesses and individuals from cyber threat. We will do this through a series of ambitious initiatives, including:

- a national extracurricular school programme to identify the most promising students with intensive

training and mentoring, starting in 2017/18 with 600 pupils in secondary schools
- establishing a range of higher and degree-level cyber apprenticeships, with tailored programmes in key sectors
- a re-training programme for people changing to cyber security mid-career

We will also:

- ensure that anyone who would do the country harm knows that we can and will fight back using the most appropriate response at our disposal, including through the use of our National Offensive Cyber Programme
- make cyberspace ‘secure by default’ by working in partnership with industry to build security into the development of the next generation of internet-connected products and services. We are establishing a project team in DCMS to take this forward
- develop international and multi-stakeholder responses to this cross-border problem, strengthening frameworks for international cooperation and developing the capacity of our partners to improve their own cyber security
- retain the trust of citizens in online public sector services and systems, ensuring that appropriate levels of security are implemented across the public sector and supporting law enforcement action to protect the public and bring cyber criminals to justice

Support for businesses and individuals

It is essential that help individuals and businesses stay safe online.

One of the UK’s best guarantees of future security is a flourishing, indigenous cyber security sector - UK companies innovating in cyber defence, keeping the UK at the sharpest edge of cyber innovation, and creating jobs and wealth in a booming market at the same time. The government has announced an interlocking series of initiatives to help grow the UK’s cyber security sector including:

- establishing two Innovation Centres in London and Cheltenham to support start-ups in the crucial first months of their development and to provide a platform for them to have access to the highest quality support
- funding HutZero, an early stage accelerator programme that provides innovators with business advice to help them take their ideas forward to commercialisation
- supporting innovators in UK universities to commercialise their ideas, through an Academic Start-Up programme
- helping UK early-stage cyber security businesses grow by sharing best practice and delivering business training ‘bootcamps’ alongside the Digital Catapult

However, we are a long way from achieving this - one in four businesses say they experienced a cyber breach in the last 12 months, yet only 22% of small businesses have provided any cyber security training to their staff.[1] So we will develop and promote guidance and schemes to help firms protect themselves against cyber threats. We will actively encourage the adoption of Cyber Essentials, our flagship, GCHQ-backed scheme which sets out the basic technical controls that all organisations, regardless of size or sector, should have in place to protect themselves against the most prevalent forms of cyber attack. We will also support public awareness initiatives, like the Cyber Aware campaign, to help raise the level of protection against cyber crime across the UK.

Finally, we will make sure that the right regulatory framework is in place in the UK, which incentivises better cyber security but avoids unnecessary business burdens. Many of our industry sectors are already regulated for cyber security, while for the wider economy the forthcoming General Data Protection Regulation is expected to drive improvements in cyber risk management due to the introduction of compulsory breach reporting and significantly increased maximum fines. We will continue to ensure the right steps are taken, particularly regarding critical national infrastructure which was recognised as a priority in the Industrial Strategy green paper, to manage cyber security risks.

Child internet safety

As well as ensuring that organisations and individuals can operate securely in cyberspace, it is also essential that children and young people are protected from inappropriate or harmful material such as extremist or age-inappropriate content.

The UK is a world leader in child internet safety, with legal protections against abuse and illegal content, and tools for parents to restrict content they do not wish their children to see. We have a strong track record in working with the internet industries to drive progress. For example, the UK Council for Child Internet Safety (UKCCIS), set up in 2008, brings the government together with key stakeholders to help keep children and young people safe online.

Recent UKCCIS achievements include:

- the roll-out of family-friendly filters for the vast majority of broadband customers, with prompts to encourage parents to activate them, and automatic family-friendly public Wi-Fi in places where children are likely to be
- guidance for providers of social media and interactive services (including gaming) to help make their platforms safer for children and young people under 18

We are always looking to do more to protect children from harm online. As a next step, the government will require age verification controls for access to online pornographic material provided on a commercial basis in the UK, which is currently easily accessible with little or no protections, to ensure that those accessing it are of an appropriate age. These measures will be backed up by a robust regulatory regime that protects children from content that can harm them.

We will continue to work in collaboration with industry, seeking to eradicate the opportunities presented by developing technology to facilitate online child sexual exploitation. The world-leading Internet Watch Foundation (IWF) was established in the UK to prevent access to images of child sexual abuse. The government has worked with the IWF to share with major technology companies almost 35,000 digital fingerprints or ‘hashes’ of indecent images of children known to law enforcement agencies, so that they can remove the images from their platforms and services.

We will also continue to lead the global effort to end online child sexual exploitation. In 2014, we set up the WePROTECT initiative, which brought together countries and international organisations, as well as major companies, in a coordinated response to the threat from online child sexual exploitation. In 2016, the WePROTECT initiative merged with the Global Alliance against Child Sexual Abuse Online to create, for the first time, a single global organisation with the influence, expertise and resources to tackle online child sexual exploitation and abuse worldwide. We have also committed £40 million to the Fund to End Violence against Children, hosted by UNICEF to further support the international effort.

And we will continue to lead the world in addressing the challenges posed by online radicalisation and extremism. Since the Counter Terrorism Internet Referral Unit was set up in 2010, it has led to the removal by companies of over 250,000 pieces of harmful terrorist and extremist content and the model is being replicated internationally.

An open internet

We will continue to work closely with international partners to ensure the continuation of a free, open and secure internet that supports our economic prosperity and social well-being.

The UK and our allies have been successful in building a broad consensus that the multi-stakeholder approach is the best way to manage the complexities of internet governance. However, there remain those who promote an alternative vision of an internet that is controlled by governments and where national borders are recreated in cyberspace. We reject such an approach and will continue to play an active role in the United Nations and other international organisations to strengthen the multi-stakeholder model and ensure that the internet remains open for technical innovation and for economic and social development around the world.

1. Cyber Security Breaches Survey 2016 _

Is there anything wrong with this page?

Services and information

Benefits

Births, deaths, marriages and care

Business and self-employed

Childcare and parenting

Citizenship and living in the UK

Crime, justice and the law

Disabled people

Driving and transport

Education and learning

Employing people

Environment and countryside

Housing and local services

Money and tax

Passports, travel and living abroad

Visas and immigration

Working, jobs and pensions

Departments and policy

How government works

Departments

Worldwide

Policies

Publications

Announcements

Help Cookies Contact Terms and conditions Rhestr o Wasanaethau Cymraeg
Built by the Government Digital Service

All content is available under the Open Government Licence v3.0, except where otherwise stated

© Crown copyright