# Press release: New measures to boost cyber security in millions of internet-connected devices

BOSSES behind ‘smart’ devices such as televisions, toys and speakers found in millions of homes will be expected to build-in tough new security measures that last the lifetime of the product, as part of plans to keep the nation safe from the increasing cyber threat.

Estimates show every household in the UK owns at least 10 internet connected devices and this is expected to increase to 15 devices by 2020, meaning there may be more than 420 million in use across the country within three years.

Poorly secured devices threaten individuals’ online security, privacy, safety, and could be exploited as part of large-scale cyber attacks. Recent high-profile breaches putting people’s data and security at risk include attacks on smart watches, CCTV cameras and children’s dolls.

Developed in collaboration with manufacturers, retailers and the National Cyber Security Centre, the Government’s Secure by Design review review lays out plans to embed security in the design process rather than bolt them on as an afterthought.

The Government will work with industry to implement a rigorous new Code Of Practice to improve the cyber security of consumer internet-connected devices and associated services while continuing to encourage innovation in new technologies.

Speaking ahead of a launch event at consumer champion Which? headquarters, Margot James, Minister for Digital and the Creative Industries, said:

> We want everyone to benefit from the huge potential of internet-connected devices and it is important they are safe and have a positive impact on people’s lives. We have worked alongside industry to develop a tough new set of rules so strong security measures are built into everyday technology from the moment it is developed.
>
> This will help ensure that we have the right rules and frameworks in place to protect individuals and that the UK continues to be a world-leading, innovation-friendly digital economy.

Dr Ian Levy, the NCSC’s Technical Director, said:

> The NCSC is committed to ensuring the UK has the best security it can, and stop people being expected to make impossible safety judgements with no useful information.

> We are pleased to have worked with DCMS on this vital review, and hope its legacy will be a government ‘kitemark’ clearly explaining the security promises and effective lifespan of products.

> Shoppers should be given high quality information to make choices at the counter. We manage it with fat content of food and this is the start of doing the same for the cyber security of technology products.

The Secure by Design report outlines practical steps for manufacturers, service providers and developers. This will encourage firms to make sure:

- All passwords on new devices and products are unique and not resettable to a factory default, such as ‘admin’;
- They have a vulnerability policy and public point of contact so security researchers and others can report issues immediately and they are quickly acted upon;
- Sensitive data which is transmitted over apps or products is encrypted;
- Software is automatically updated and there is clear guidance on updates to customers;
- It is easy for consumers to delete personal data on devices and products;
- Installation and maintenance of devices is easy.

Alongside these measures for ‘Internet of Things’ manufacturers, the report proposes developing a product labelling scheme so consumers are aware of a product’s security features at the point of purchase. The Government will work closely with retailers and consumer organisations to provide advice and support.

Alex Neill, Which? Managing Director of Home Products and Services, said:

> With connected devices becoming increasingly popular, it’s vital that consumers are not exposed to the risk of cyber-attacks through products that are left vulnerable through manufacturers’ poor design and production.

> Companies must ensure that the safety of their customers is the absolute priority when ‘smart’ products are designed. If strong security standards are not already in place when these products hit the shelves, then they should not be sold.

Julian David, CEO of TechUK said:

> The opportunities created by the Internet of Things are now becoming clear. It offers consumers and citizens greater empowerment and control over their lifestyles, from managing energy consumption at home to having peace of mind that a frail relative is going about their normal routine.
>
> However, these opportunities also bring risk and it is important that the IoT market now matures in a sensible and productive way, with security embedded at the design stage. This project is the start of that maturity. Industry has been keen to engage in the review and demonstrate what is best practice. It is important that companies throughout the supply chain now adopt and build on this Code of Practice to build the trust required to drive widespread take-up of the IoT.

Mark Hughes, CEO, BT Security:

> BT shares the Government's ambition to make the UK the safest place to work and do business online. We are proud to have played a key advisory role in the development of the draft Code of Practice, having shared our technical insight with the Government in our capacity as a global network operator, UK broadband provider and as a global provider of cyber security and IoT services.
>
> From the development of the world's first Cleanfeed filter to block child abuse images, free parental controls for broadband products and devices, to warning or blocking our customers from known malware and phishing sites, BT has been at the forefront of keeping consumers and families safe online for many years. BT is actively involved in driving standards, interoperability and security across the IoT market and will continue to provide guidance to the Government and industry around best practice for securing internet connected devices.

This initiative is a key part of the Government's five-year, £1.9 billion National Cyber Security Strategy which is making the UK the most secure place in the world to live and do business online.

## Notes to Editors

The Secure by Design report was developed by DCMS in conjunction with the National Cyber Security Centre and with support from other Government departments, industry and academic partners. The project has been informed by

an expert advisory group which included subject matter experts from industry, consumer organisations and academia. The report can be found at Secure by Design report.

Stakeholders have an opportunity to send feedback on the report's draft proposals via securebydesign@culture.gov.uk from the 7th March until the 25th April.

The Government's Digital Strategy includes the aspiration for the UK to remain an international leader in the development and uptake of IoT. The Government's actions include the funding of research and innovation in IoT, including through three-year £30 million IoT UK Programme.

The Government's Digital Charter is a rolling programme of work to agree norms and rules for the online world and put them into practice. In some cases this will be through shifting expectations of behaviour; in some we will need to agree new standards; and in others we may need to update our laws and regulations. Our starting point will be that we will have the same rights and expect the same behaviour online as we do offline.

**Consumer tips for IoT device security:**

- Research the security of a product before buying
- Check your home router does not have a default password/username
- Change any default passwords and usernames found in devices
- Check all the available security settings
- Check the manufacturers' website to see if there are any updates available
- If there's a two-step identification option – use it

Further guidance on security for consumer IoT / devices can be found ICO's website.

Associated services: This primarily refers to applications that manage internet-connected devices. Such applications usually run on phones and connect to cloud-based services.

Draft Code of Practice:

- All IoT device passwords must be unique and not resettable to any universal factory default value.
- Companies that provide internet-connected devices and services must have a vulnerability disclosure policy and point of contact.
- Software must be kept updated. This includes the need for updates to be timely and not impact on the functioning of the device
- Any credentials must be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable
- Security-sensitive data, including any remote management and control, should be encrypted when transiting the internet, appropriate to the properties of the technology and usage. All keys should be managed securely
- Ensure software integrity: Software on IoT devices must be verified

using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function
- Ensure that personal data is protected in accordance with data protection law
- Make systems resilient to outages. Resilience must be built into IoT services where required by the usage or other relying systems, so that the IoT services remain operating and functional
- Monitor system telemetry data. If collected, all telemetry such as usage and measurement data from IoT devices and services should be monitored for security anomalies within it
- Make it easy for consumers to delete personal data on devices and products.
- Make installation and maintenance of devices easy
- Validate input data: Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices must be validated

The Government will be conducting more work in 2018 to further develop these recommendations. This will involve considering how following the Data Protection Bill, the Government can further embed guidelines in the Code of Practice within regulations.

This initiative is a key part of the Government's five-year, £1.9 billion National Cyber Security Strategy which is making the UK the most secure place in the world to live and do business online.

---

# Press release: International Women's Day: Penny Mordaunt pays tribute to Jo Cox and calls for gender equality to be made a reality

Jo Cox pictured working as a humanitarian aid worker. Photo: Oxfam

International Development Secretary Penny Mordaunt has paid tribute to MP Jo Cox's humanitarian work and called for everyone to "raise their game" to make gender equality a reality, ahead of this year's International Women's Day.

Speaking today (7 March) at the headquarters of mobile technology industry association the GSMA, in the City of London, Ms Mordaunt will announce new UK aid support to help grassroots organisations working on issues that were close to Jo's heart.

Ms Mordaunt will also call for everyone to step up and make gender equality a reality, as part of the Department for International Development's (DFID) new vision to make sure the voices of women and girls in the world's poorest countries are heard.

The International Development Secretary will say that if progress on gender equality is not sped up, the Global Goals will not be met by 2030.

## Ahead of her speech, International Development Secretary Penny Mordaunt said:

> Jo was a dedicated humanitarian who fought for gender equality at home and in developing countries and her passion and commitment will continue to support the world's most disadvantaged and disenfranchised women through these new UK aid grants.
>
> The MeToo movement has sent shockwaves around the world and given a voice to millions of women, but the majority of women and girls in the poorest countries are still not heard.
>
> We all have the power to change this injustice and that's why UK aid is keeping girls in school, stamping out violence and giving a voice to women both at home and in shaping the future of their countries.
>
> It is only by everyone raising their game and making gender equality a reality that we will build a more peaceful, safe and prosperous world for us all.

The Jo Cox Memorial Grants will be given to projects in developing countries that are working to get the voices of girls and women heard when holding power-holders to account, helping them find jobs and become financially independent and making access to family planning services easier. The fund will also help strengthen grassroots organisations' capacity for predicting identity-based violence earlier.

## Jo Cox's sister Kim Leadbeater said:

> It's wonderful to have the Jo Cox Memorial Grants being launched today – for every life that is touched by these grants, they will make a real difference and they will be money well spent.
>
> It's so fitting to have these grants created in Jo's name, which will reach a range of different countries and projects that encompass Jo's passion for both women's empowerment and bringing local communities together.
>
> Jo spent 20 years working in the voluntary sector and working overseas. These grants are a reminder of that and a reminder of her passion and her determination to hopefully inspire others with

similar desires. Jo would be over the moon.

In her speech, Ms Mordaunt will set out that DFID has taken the lead in tackling sexual abuse and exploitation within the aid sector and acknowledge that these incidents would not be so widespread if women and girls had an equal place at the table.

There are three areas in Ms Mordaunt's call to action that DFID will focus on through the new Strategic Vision for Gender Equality:

- Reaching those women and girls most at risk of being left behind, whether that is because of their ethnicity, their disability or simply because of where they are.

- Stepping-up for women and girls caught-up in conflict or crisis. To ensure that as well as protecting them, women and girls are also empowered, so they have a seat at the table when it comes to finding the solutions to a lasting peace. Studies show that when women are at the negotiating table, peace treaties are a third more likely to work.

- Doing more to increase women and girls' political participation so their voices are heard, and they're able to influence decisions that affect their lives, whether that's at home or in government.

Ms Mordaunt will deliver her speech at GSMA to highlight that technology will be vital in making sure the voices of women and girls in the world's poorest countries are heard.

DFID is supporting the GSMA to narrow the gender gap on mobile phone ownership in order to unlock the benefits that mobile and internet can bring, for example giving women access to financial services, educational resources and digital health services.

## Jo Cox Memorial Grants:

## Gender data:

- Ms Mordaunt will also today announce funding for the UN Women-led flagship programme initiative on gender data, to improve the quality of gender data so the global goals can be effectively monitored. UK aid support will be up to £6 million over 4 years.

## New Strategic Vision for Women and Girls:

- The new Strategic Vision re-affirms the UK's position as a world leader on gender equality. Focuses of the vision include strengthening work on gender equality in conflict and crisis contexts, women's political empowerment, and ensuring that no women or girls are left behind. It is an update of DFID's 2011 Strategic Vision for Girls and Women. DFID has

compiled the new vision after a process of wide consultation with NGOs and civil society, both in the UK and abroad.

**GSMA:**

- Specifically DFID is supporting women and girls through the GSMA by working with the mobile industry to ensure their services are designed with women and girls in mind. For example in Rwanda the local mobile operator is training and employing female Mobile Money agents, who are better able to reach women with financial services, allowing them to save money and support their families.

---

# Press release: UK charities commit to strengthening safeguarding culture and capability

UK charities have today committed to strengthening their leadership, culture and capacity around safeguarding.

The pledge was made at a summit in London this morning (Tuesday), hosted by the Charity Commission and the Office for Civil Society at the Department for Digital, Culture, Media and Sport. The summit brought charities working in the UK together with their regulators and other agencies, as well as independent safeguarding experts, and focused on setting out the specific safeguarding challenges facing charities working in the UK. It followed a summit on Monday, focused on charities working internationally.

Attendees acknowledged the impact on public trust in charities from the recent revelations around sexual exploitation by individuals involved in international aid agencies. They committed to working together to lead a meaningful response to safeguarding concerns facing the domestic charitable sector, and to achieve the highest standards of safeguarding.

Themes agreed for priority action were:

- leadership, culture and values
- law, regulation and the statutory framework
- capacity and capability in charities around safeguarding and
- responsibilities and reporting, accountability and transparency.

### Helen Stephenson, Chief Executive of the Charity Commission, said:

Keeping people safe must be the top priority for all charities,

> wherever they work and whatever they do – the public, rightly, expect all charities to be safe places for those who come into contact with them. Sadly, concerns about safeguarding in charities are not limited to international aid organisations. Charities working in the UK have their own safeguarding challenges that must be addressed. I am encouraged by the commitment shown today by UK charities to lead and drive improvements around safeguarding. That commitment must be followed by firm action, and we as regulator will work with and support charities in developing practical, workable changes.

### Minister for Civil Society, Tracey Crouch, said:

> Safeguarding must be at the heart of every charity's culture and a central priority for its leadership. I have been clear to the sector that they must make safeguarding a key priority. It is crucial that the sector addresses this issue urgently to protect vulnerable people and rebuild the public's trust.

The summit was chaired by Professor John Drew CBE, former chief executive of the Youth Justice Board, and author of a review into South Yorkshire Police's handling of child sexual exploitation.

Attendees agreed to develop action plans for each of the themes and reconvene in two months' time, to commit to implementation and discuss early progress in delivering change. Charity regulators in Scotland and Northern Ireland will be leading their own action plans. This work will feed into a wider safeguarding conference planned for later in the year.

The Charity Commission this week confirmed that reports of serious incidents on safeguarding have nearly doubled since revelations of sexual exploitation by Oxfam staff in Haiti emerged at the beginning of February. The regulator has established a new taskforce to deal with increased serious incident reports, and to undertake proactive work to ensure prompt and full reporting of serious safeguarding incidents by charities. That taskforce is also undertaking a 'deep dive' of existing serious incident reporting records to ensure any gaps in full and frank disclosure are identified and responded to.

### Ends

### Notes to editors:

1. The Charity Commission is the regulator of charities in England and Wales; charities in Scotland are regulated by the Office of the Scottish Charity Regulator and charities in Northern Ireland are regulated by the Charity Commission for Northern Ireland. All three regulators took part in the summit.
2. Among the charities and organisations attending the UK safeguarding summit were NCVO, ACEVO, SCVO, Association of Chairs, Small Charities

Coalition, Scouts Association, Alzheimer's Society, Barnado's, Scouts Association, The Children's Society, Children in Need, NSPCC, Age UK, Big Lottery Fund, Managing Together Ltd, Bond, Children England, the Charity Retail Association.

3. On 17 February, the Commission set out a range of new measures on safeguarding.

---

# News story: Crown Prince Mohammed bin Salman of Saudi Arabia's visit, March 2018

Britain's relationship with one of our oldest friends in the Middle East will begin a new chapter with the visit of Saudi Crown Prince Mohammed bin Salman

His Royal Highness Mohammed bin Salman is visiting the UK for the first time since he became Crown Prince in June 2017 and since Saudi Arabia started a major programme of domestic reforms. Saudi Arabia is amongst the largest political, diplomatic and economic power in the Middle East, and the visit will usher in a new era in our bilateral relations with one of our oldest friends in the region.

The Crown Prince's visit builds on the Prime Minister's visit to Saudi Arabia in November 2017. It will help to enhance our co-operation in tackling international challenges such as terrorism, extremism, the conflict and humanitarian crisis in Yemen and other regional issues such as Iraq and Syria.

Saudi Arabia has also set out Vision 2030, a roadmap to open up the country's economy over the next 15 years. This will provide opportunities for British businesses in sectors including education, entertainment and healthcare where they have world-class expertise. It also includes plans for Saudi Arabia to become a global investment powerhouse and the Crown Prince's visit will help explore ways in which Saudi Arabia can build on its investment in the UK in sectors such as infrastructure.

## British Ambassador Simon Collis talks about the ties between our two countries

Saudi Crown Prince Visit

## Find out more about the Crown Prince's visit

Published 6 March 2018

---

# News story: Penny Mordaunt's statement on Eastern Ghouta

I am appalled that yesterday's joint aid convoy into Eastern Ghouta was forced to halt its critical life-saving work because of continued airstrikes in civilian areas by the Asad regime.

Yesterday's incomprehensible actions by this brutal dictator, removing over 70% of everyday medical supplies for innocent families including vital insulin and dialysis equipment, serves purely to inflict as much misery as possible onto the Syrian people.

These actions have needlessly put thousands of lives at risk – some of those trapped and in need of urgent medical care will die unless all parties, including Russia, respect the 30-day ceasefire in Syria and allow unrestricted humanitarian access and the evacuation of the critically sick and wounded.