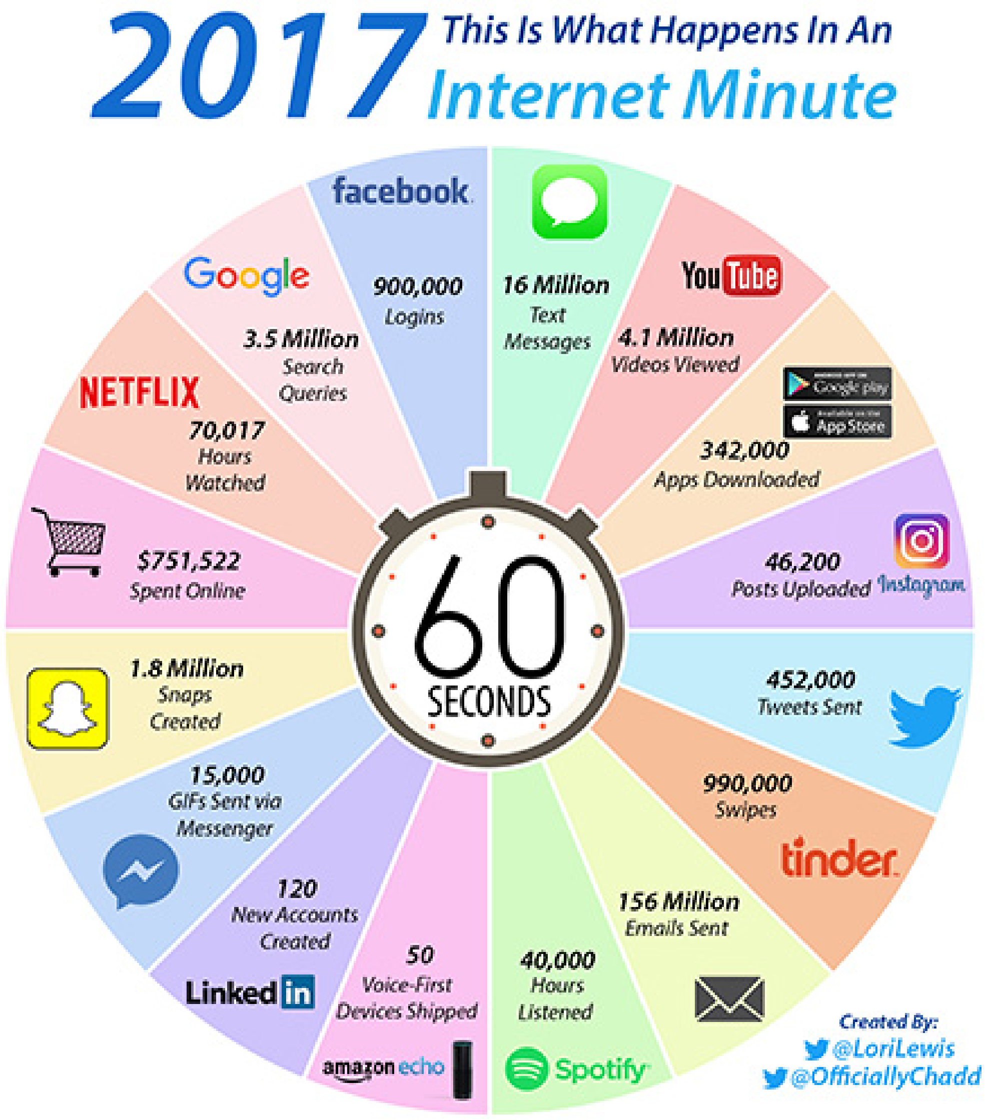
Thames Valley
Community Safety Partnerships’

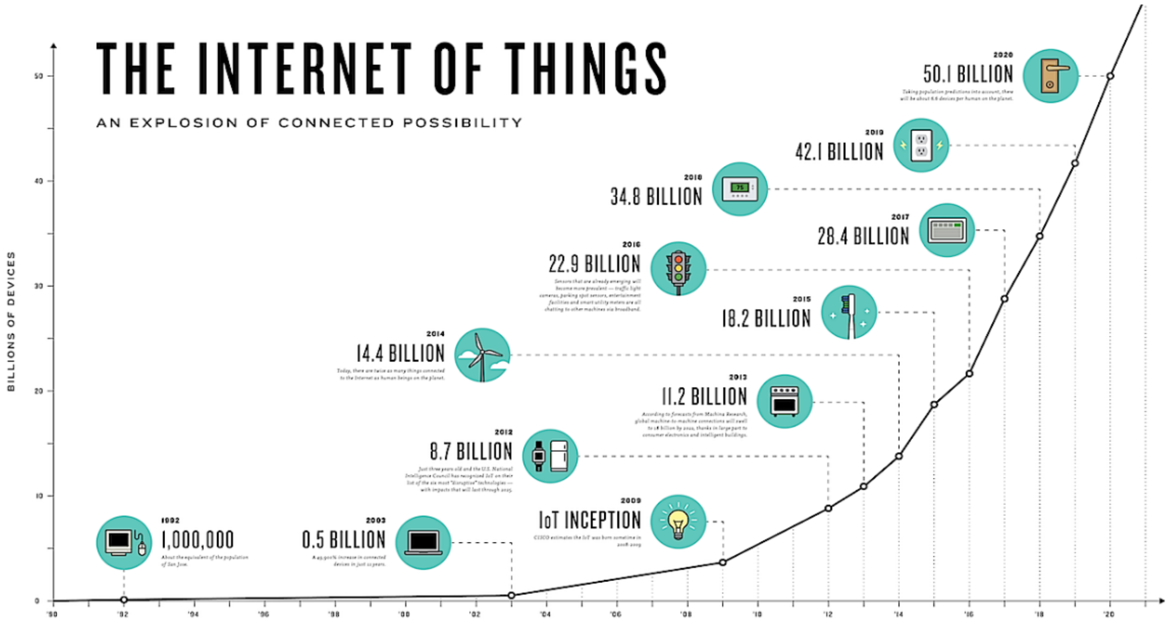
Cyber / Digital Crime Strategy
2017-2020



Introduction

Cyber / Digital crime is an international challenge as the internet has removed the protective barrier of national and local borders and, in many cases, the protective barrier of individual homes and businesses.

Additionally, more and more people across the UK are connected to the internet via multiple devices and across all age ranges.



The National Crime Agency (NCA) estimates that the cost of cyber-crime to the UK economy is billions of pounds per annum and growing.

International and domestic cyber criminals increasingly view UK-based businesses and private individuals as attractive targets.

The Crime Survey for England & Wales 2017 highlighted:

- 2.0 million Computer Misuse offences, the majority malware.
- 24% involved a loss, all related to malware.
- The majority of victims (87%) had only been a victim once.
- Of the separate 3.6 million fraud offences, 1.9 million were cyber-related.

The Office of National Statistics (ONS) estimated 5.8 million incidents of fraud and computer crime were experienced by adults in England and Wales in 2016. This exceeds the total volume of recorded crime across the whole of England & Wales in the same period.

Under-reporting by organisations and individuals is common; therefore we do not know the full scale of the cyber-crime threat to the UK.

Aim & Scope

This strategy deals with cyber-crime in the context of two interrelated forms of criminal activity:

1. **Cyber-dependent crimes** – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. phishing emails, spyware, destroying data or networks)
2. **Cyber-enabled crimes** – 'existing' crimes which have been transformed in scale, form or reach by the use of computers, networks and the internet or other forms of ICT (e.g. harassment, fraud, grooming)

The aim of this strategy is to bring together Community Safety partners across the Thames Valley Police force area to:

- improve the awareness of digital / cyber risk and vulnerability in our communities
- improve the resilience of our communities to this fast evolving area of crime through access to information, tips, tools and better practises for all
- deter people from becoming involved in the criminal aspects of online behaviour
- pursue a common approach to cyber-crime by maintaining collaboration across the Thames Valley area
- ensure consistent advice and accurate messages are being delivered across our collective engagement mechanisms (e.g. campaigns, social media etc)

Joined up Partnership Approach

The Police and Crime Plan 2017-21

What crimes cause the most concern in Thames Valley?

- 3,476 Adults Surveyed – cyber-crime was the fourth highest concern (below burglary, violence and sex offences)
- 1,215 Young individuals Surveyed (Aged 11 – 17) – young females were most concerned about bullying (verbal and cyber), sexting and unwanted sexual comments or jokes.

The Police & Crime Commissioner has placed Cyber Crime within the "Prevention and Early Intervention" priority area of his Police and Crime Plan 2017-21, with the key aim to:

> *"Support coordinated efforts by police and partner agencies to improve public awareness of measures to protect themselves from cybercrime, particularly targeting those most at risk (such as those at either end of the age spectrum)".*

As Community Safety Partnerships (CSPs), we will align our activity with the Government's '4 Ps' agenda for Serious & Organised Crime:

- PURSUE: Prosecute and disrupt people engaged in cyber crime
- PREVENT: Prevent people from engaging in cyber crime
- PROTECT: Increase protection against cyber crime
- PREPARE: Reduce the impact of this criminality where it takes place.

The skills, reach and expertise of CSPs mean that we are best placed to directly impact TWO of the ‘4 Ps’:

PREVENT
Focused on reaching people who may not understand the consequences of their actions, and deter those who may have committed cyber-crimes from further criminality

PROTECT
Focused on traditional crime prevention models, looking at how to help increase people’s cyber security for themselves and others, particularly the most vulnerable

The UK Government cannot do this alone. Every individual, business and organisation must play their part in protecting themselves and others from cyber-crime. Community Safety Partnerships are well placed to support this approach to cyber-crime through engagement and provision of advice.

Key areas of focus

The Community Safety Partnerships across the Thames Valley have come together to recognise that online crime does not respect geographic boundaries and that working together is an effective way to tackle this growing issue.

There are key areas of focus which are shared across the Thames Valley area and these include (not in priority order):

1. **Exploitation of children and young people** (e.g. grooming, sexting etc)
2. **Exploitation of adults and vulnerable or targeted groups** (e.g. fraud/scams etc)
3. **Abuse and Violence** (e.g. hate crime, harassment, bullying etc)
4. **Online Radicalisation** (e.g. terrorism etc)
5. **Business Resilience** (e.g. attacks on business for financial gain or to disrupt organisations)

What we know

1. Exploitation of children and young people

More than four in five young people aged 5–15 are now able to access the Internet in their own homes, with just over a third of 12-15 year olds and 15% of 8-11 year olds able to access the Internet in their bedrooms. The amount of time children spend online has doubled since 2005, with 5-16 year olds now spending an average of 3 hours per day; this rises to nearly 5 hours for 15-16 year olds (Ofcom, 2015).

This access to young people compromises the protection that physical boundaries and guardians have over them.

The Internet Watch Foundation (IWF) is a global and independent organisation that removes reported images of child sexual abuse. This includes what they call Category A images (penetrative sexual activity including rape or torture). In 2016 they received 57,335 reports which were confirmed as child sexual abuse:

- 45% of the 'victims' were 11-15 years
- 53% were aged 10 and under
- 2% were aged 2 and under
- 89% of images were girls
- 28% were Category A images

To put it into context, every five minutes the IWF assesses a webpage and every nine minutes that webpage shows a child being sexually abused.

The top two host countries are the Netherlands and the USA. Notably the USA has only recently dropped to second with an 18% increase in the Netherlands, meaning the hosting problem is closer to the UK than ever before. Since the IWF began to tackle this issue the problem in the UK has dropped from 18% (in 1996) to 0.1% in 2016. While the UK may not produce as much content, they remain a large 'consumer'.

Services that support children who are victims have seen a marked increase in online crime. In 2015, ChildLine saw a 168% increase in counselling sessions related to online sexual abuse. Grooming and sexting have increased with the reported ages of children affected getting younger.

2. Exploitation of adults and vulnerable or targeted groups

The impact of cyber-crime has not just affected children and young people. Adults, whether they are perceived to be 'vulnerable' or not can place themselves at risk of a variety of issues. Traditional crimes of stealing (e.g. theft from a person or house burglary) are generally reported to the police and have seen decreases across the country as police and partners better understand and tackle those crimes.

In contrast, crimes of grooming, fraud, phishing, online scams, revenge pornography, stalking, and harassment are on the rise. Much of this criminality is unreported, unrecorded and as a result not fully understood.

From November 2015 to Feb 2016 a South East cyber-crime survey[1] was completed by 11,600 people.

- 84% of people had experienced some form of 'attempted' cyber-crime in the previous 12 months, especially fraudulent emails.
- People reported that they fell victim most often to Phishing Scams[2], followed by Online Banking fraud

[1] South-East CyberCrime Survey for adults in Surrey, Hampshire, Sussex, Kent and Thames Valley

[2] Phishing is an attempt at identify theft in which criminals lead users to a counterfeit website in order to deceive the user into parting with personal information or money

- 29% of people had some form of financial impact with the majority losing between £100 and £500
- People aged between 18-44 were least likely to report that they had been a victim and only 31% of victims reported the offence to relevant authorities

Fraud can be an even greater threat to adults who are vulnerable due to lack of support, lack of knowledge or lack of protective factors (as seen with learning and other disabilities). In 2013/14 the National Fraud Investigation Bureau identified that 70% of fraud involved a "cyber element".

3. Abuse and Violence

Abuse and violence (whether in a community or domestic setting) has seen an increase over the past two years. Some believe that it is merely an increase in reporting and others are concerned that there is also an increase in real terms. Violence is not only about physical harm but includes the crime of "violence without injury", examples of which are threats to kill, intimidation, harassment, bullying and hate crime.

The internet, social media in particular, has enabled people to be targeted with this violence without injury as the perpetrator is often able to remain anonymous and does not need the "courage" to cause this distress face to face.

In many cases, especially among young people, there is a lack of awareness that this is even a crime and there is a lack of recognition about the level of harm it can cause.

It is not a new issue. In 2011 a large scale study of 11-16 year olds found that [3] 28% of 11-16 year olds reported that they have been targeted by some form of cyberbullying. Of these, one quarter experienced this as persistent over time.

4. Online Radicalisation

Radicalisation is an extremely complex area but there is increasing recognition that, although terrorism (such as that of Islamic Extremism) often involves the movement of people to and from the UK to train, there is an emergence of ways to be radicalised online.

A national survey of 11-24 year olds conducted by the National Counter Terrorism Policing HQ in 2015 highlighted that young people are heavily influenced by the content they see online - and particularly social media[4].

The police are active in tackling online radicalisation and many extremist websites are removed by the Counter Terrorism Internet Referral Unit (CTIRU). During an average week, the CTIRU is removing over 1,000 pieces of content that breach terrorism legislation.

[3] http://childnetsic.s3.amazonaws.com/downloads/Research_Highlights/UKCCIS_RH_31_Virtual_violence_II_pupils.pdf

[4] https://www.gov.uk/government/publications/online-radicalisation/online-radicalisation

Approximately 800 of these are Syria and Iraq related and have been posted on multiple platforms.

Far-Right extremist groups are also using the internet to recruit from the younger generation. It is also facilitating the ability of Far-Right groups to organise and promote themselves. Britain First has 1.8 million likes, for example. Far-Right groups have gained incredible popularity online with the internet helping them to mobilise support and recruit new members.

5. Business Resilience

"Last year, the average cost of breaches to large businesses that had them was £36,500. For small firms the average cost of breaches was £3,100. 65% of large organisations reported they had suffered an information security breach in the past year, and 25% of these experienced a breach at least once a month. Nearly seven out of ten attacks involved viruses, spyware or malware that might have been prevented using the Government's Cyber Essentials scheme."
2016 Government Cyber Health Check and Cyber Security Breaches Survey

Organisations of all types and sizes have been victims of cyber-attacks. The CSPs across the force area recognise the need to support our small and medium businesses (SMEs) who may not have the level of assistance or access to support that some larger corporations do.

- 3.9 million cyber-crimes were reported in 12 months (2016)
- This is up from 2.5 million in 2015
- 28% of businesses reported attacks to Police
- Around 1 in 3 small businesses experienced a cyber breach / attack in 2015/16 (Cyber Security Breaches Survey 2016)
- Estimated cost to UK economy: £27 Billion in 2011 → £49 Billion in 2014 and rising
- An average data breach costs £1.46M to £3.14M (large company)
- 500 million new viruses in 2015
- 3,000 DDoS (denial of service) attacks per day
- 500,000 phishing attempts per day (93% of it ransomware)

(source: Thames Valley Police, except where noted)

As organisations increasingly move to flexible working arrangements where employees can work remotely or Bring Your Own Device (BOYD), the protection of the organisation can be lost or diminished.

Employees themselves have been involved in attacks on their own organisation. "Corporate employee fraud – where employees or ex-employees obtain property or compensation through fraud, or misuse corporate cards and expenses – is also on the rise, with 1,440 cases recorded in 2015 – 2016. Listed in the top 10 most reported crimes by businesses in the past 12 months, this demonstrates how fraud is not just an external threat, but can also affect a business from the inside." (Computer Weekly, June 2016)

Tackling cyber-crime is everyone's responsibility…

Government Communications Headquarters (GCHQ) estimates that 80% of cybercrimes are preventable by implementing simple safety measures, such as virus protection alongside strong and secure passwords. They assert that raising awareness among young people, parents and other vulnerable adults on the potential dangers are primary methods to reduce risk. In combination with this, we aim to provide the tools and information to enable people to act on the warnings they receive as this reduces fear and gives individuals more control over their safety.

We are keen to ensure that the messages being shared about how to keep yourself safe are consistent across the Thames Valley and even nationally. To that end, we have maintained contact with the National Crime Agency's 'National Cyber Crime Unit', known as the NCCU.

What the Government are doing

The NCCU is a central Government established single, central body for cyber security at a national level. This body manages national cyber incidents, provides an authoritative voice and centre of expertise on cyber security, and delivers tailored support and advice.

The National Cyber Security Centre (NCSC) launched on 1 October 2016. It was set up to help protect our critical services from cyber-attacks, managing major incidents and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations.

Some of this defensive activity is automated, such as with the Active Cyber Defence (ACD) programme which launched in November 2016. The ACD programme is intended to tackle, in a relatively automated way, a significant proportion of the cyber-attacks that hit the UK.

This is just some of the Government's activity. Further information can be obtained from the NCCU and NCSC websites:

- http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit
- https://www.ncsc.gov.uk/

What Community Safety Partnerships are doing

Here in the Thames Valley, this strategy aims to set out a shared approach to tackling cyber-crime and enable people and businesses to protect themselves. Our work to protect communities places local support behind the key messages and advice for individuals and businesses.

The National Cyber Crime Unit have worked hard on key campaigns called Get Safe Online' and 'Cyber Aware' which provide public advice messages for everyone to help protect themselves against the majority of attacks. CSPs are working hard to deliver these messages at every opportunity and would signpost most residents to these two websites:

- https://www.getsafeonline.org/
- https://www.cyberaware.gov.uk/

Where there are audience groups that would benefit from specific information, such as children, older people or those with additional needs, we are delivering both face to face sessions and advice through existing communication methods, including Thames Valley Alert, social media and traditional media. We are also making use of existing networks who already work with those groups, whether that be schools or the voluntary sector.

Our prevention work aims to deter people who could be, or are, drawn into cyber criminality. It also aims to publicise when disruptions are successful and tackle the desire to enter into this crime while dealing with the misperception of cyber-criminality as desirable. Making people aware of the consequences and penalties is one approach to this.

What Businesses can do

There are nationally developed resources for Businesses which include:

- CYBER ESSENTIALS: Basic advice to protect your business from majority of cyber attacks
- 10 STEPS TO CYBER SECURITY: Further guidance on how to protect from cyber-crime aimed at larger organisations
- CYBER INFORMATION SHARING PARTNERSHIP (CISP): Online platform to share information between businesses, NCSC and law enforcement, with forums based on sectors and regions.

What You can do

As indicated previously, cyber-crime is hugely under-reported and the lack of information means that it is a struggle for the relevant authorities to fully understand the problem and assess risk.

Action Fraud is the UK's national fraud and cyber-crime reporting centre. Anyone can call the reporting center on 0300 123 2040. The easiest way to report fraud and cyber-crime is by using their online reporting tool: https://www.actionfraud.police.uk/report_fraud.

Anyone who wishes to remain anonymous can also report the crime to Crimestoppers who are an independent charity by calling them on 0800 555 111.

The best way to protect yourself from being a victim of any kind of cyber-crime, however, is to follow the up to date and expert advice given at:

- https://www.getsafeonline.org/ and
- https://www.cyberaware.gov.uk/

The information helps to protect yourself, your devices, your data, your money and your family.

Further resources are available at the end of this document, as an appendix.

ActionFraud

Report Fraud & Internet Crime

actionfraud.police.uk

ChildLine

0800 1111 ☎

THINK
U
KNOW
.co.uk

Childnet
International

GET
SAFE
ONLINE
.org
TM

Appendix - Cyber Prevention Resources by audience type

Young People

Online grooming

- NSPCC Share Aware campaign - 'I saw your willy' (https://youtu.be/sch_WMjd6go) and 'Lucy and the Boy' (https://youtu.be/kwcL-VP3FYc). These films can also be used as lesson discussion starters with older young people and with parents and carers. Both deal with the issue of sexting and show the risks of sharing online.

- CEOP ThinkUKnow – video and awareness resources categorised by age range from 5 to 14 plus - https://www.thinkuknow.co.uk/

- NSPCC – information and guidance for young people as well as parents and carers - https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/grooming/

- Kayleigh's Love Story – real life case study of 14 year old Kayleigh Haywood who was groomed online and then murdered - https://leics.police.uk/categories/kayleighs-love-story-film

- Murder Games – BBC documentary on online gaming and the grooming of Breck Bednar - http://www.bbc.co.uk/programmes/p03cgtx5

Sexting

- So You Got Naked Online – This is a resource that offers children, young people and parents advice and strategies to support the issues resulting from sexting incidents - http://swgfl.org.uk/products-services/esafety/resources/So-You-Got-Naked-Online.

- Romeo and Juliet (ThinkuKnow) -This short film, aimed at parents and carers, puts a modern twist on the story of Romeo and Juliet showing how the lives of these young lovers might play out online today - https://www.thinkuknow.co.uk/parents/Romeo_and_Juliet/

- Nude Selfies (ThinkuKnow) - 4 short animations that support parents and carers to have conversations with their children - https://www.thinkuknow.co.uk/parents/article-repository/Nude-selfies-a-parents-guide/

- NSPCC advice for parents and carers on Sexting - https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

- Thames Valley Police 'Amy's Story' true life case study video https://www.youtube.com/watch?v=GQDBX1nZ2U8

- Childline 'Zip It' App – website full of hints and tips to help you stay in control of online chat - https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/zipit-app/

- Sexting in Schools and Colleges: Responding to incidents and safeguarding young people – advice for schools and other professionals working with young people on how to respond to Sexting incidents - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

Cyber bullying

- Childnet International Cyber Bullying Guidance for Schools - http://www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters – enables parents and carers to 'Learn about it, how to protect your child and how to deal with it' https://www.internetmatters.org/issues/cyberbullying/?gclid=CLuKsdfAqdQCFewV0wodBjwIMw

- Cyber Bullying Teaching Resources – TES resources including links to advice articles, an ICT lesson resource and information about the risks of Cyber Bullying - https://www.tes.com/articles/cyberbullying-teaching-resources

Online Radicalisation

- Internet matters – advice for parents and carers on the online radicalisation of young people - https://www.internetmatters.org/issues/radicalisation/

General

- Disrespect Nobody – Government website for young people covering Sexting, relationship abuse, consent, rape and pornography. Contains short film clips that could be used as lesson/discussion starters - www.disrespectnobody.co.uk

- Social Media Checklists (South West Grid for Learning) – Checklists including guidance for Facebook, Instagram, Snapchat and Twitter - http://swgfl.org.uk/magazine/6-steps-to-understanding-snapchatc

- That's Not Cool – advice on healthy relationships and digital dating abuse - https://thatsnotcool.com/

- Online Reputation Checklist – simple checklist to help manage and maintain your online reputation - http://www.childnet.com/resources/online-reputation-checklist

- Smartie the Penguin – e-Safety story for 3 to 7 year olds - http://www.childnet.com/resources/smartie-the-penguin

- Digiduck's Big Decision – e-Safety story for 3 to 7 year olds on a story of friendship and responsibility online - http://www.childnet.com/resources/digiducks-big-decision

- Crossing the Line – a PSHE Toolkit covering Sexting, Cyber-bullying, Peer Pressure and Self-Esteem - http://www.childnet.com/resources/pshetoolkit

- South West Grid for Learning 360 Degrees Safe – an overview to ensure that school settings have appropriate safeguarding in place in regards to e-Safety as outlined in the Ofsted Framework - http://www.360safe.org.uk/Home

- UK Safer Internet Centre – Helpline for Professionals - https://www.saferinternet.org.uk/professionals-online-safety-helpline

For parents

- Guidance for Parents: Supporting young people online – Information for parents and carers on supporting young people online (also available in various languages) - http://www.childnet.com/ufiles/Supporting-young-people-online.pdf

- ThinkUKnow – Online safety resources for parents and carers including more information about keeping your child safe online as well as providing guidance on where you can report any concerns - https://www.thinkuknow.co.uk/parents/

- Learning Disabilities, Autism and Internet Safety: A Guide for Parents – this guide outlines some suggestions to help parents carers with children who have learning disabilities - https://www.mencap.org.uk/sites/default/files/2016-11/Internet-Safety-web-2016.pdf

- NSPCC advice for parents and carers on Sexting - https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

- NSPCC – information about setting up parental controls - https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/parental-controls/

- NSPCC Net Aware – guide for parents and carers on the social media that their children use - https://www.net-aware.org.uk/

- NSPCC and O2 Helpline for parents - https://www.nspcc.org.uk/what-we-do/about-us/partners/nspcc-o2-online-safety-partnership/

- National Crime Agency – Cyber Choices campaign to prevent young people from becoming Cyber Criminals - http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved

Small Businesses

- Thames Valley Police Protect Your World case study videos for small businesses - http://releasd.com/9703/protectyourworld-stay-safe-online-campaign

- 'Little Book of Big Scams: Business Edition' - https://www.thamesvalley.police.uk/documents/1137/the-little-book-of-big-scams.pdf

- Get Safe Online advice page for businesses - https://www.getsafeonline.org/business/

- National Cyber Security Centre Guidance on Ransomware - https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

- Cyber Essentials – shows you how to put technical measures in place to protect your business against the most common internet threats - https://www.cyberaware.gov.uk/cyberessentials/

- Home Office – Free online Cyber Security training for businesses including specific guidance for various industries such as HR, Procurement and Accountants - https://www.gov.uk/government/collections/cyber-security-training-for-business

- The Cyber Security Incident Response Scheme – provides details of certified companies that can help businesses after a Cyber attack - https://www.ncsc.gov.uk/information/crest-cyber-security-incident-response-csir-scheme

- The Cyber Security Information Sharing Partnership – enables businesses to share information on Cyber threats, get Government threat alerts and discuss security issues via a secure online platform https://www.ncsc.gov.uk/cisp

- 'Ten Steps to Cyber Security' –guidance on how organisations can protect themselves in Cyber space, including the ten steps to Cyber Security - https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

- 'Small Business: What You Need to Know About Cyber Security' – this guidance explains the threat from Cyber attack and shows how you can protect your business - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf

General

- Thames Valley Police Protect Your World content including case study videos, awareness posters and leaflets - http://releasd.com/9703/protectyourworld-stay-safe-online-campaign

- The Little Book of Cyber Scams - https://www.thamesvalley.police.uk/about-us/publications-and-documents/little-book-cyber-scams/

- The Little Book of Big Scams - https://www.thamesvalley.police.uk/about-us/publications-and-documents/little-book-big-scams/

- Cyber Aware – UK National Cyber Crime prevention advice website - https://www.cyberaware.gov.uk/, including toolkit of leaflets and other resources - https://www.cyberaware.gov.uk/toolkit

- Action Fraud Alerts – sign up to Action Fraud to receive regular alers on current fraud and online scams - www.actionfraud.police.uk/support-and-prevention/signup-to-action-fraud-alert

- Age UK – Guide for Internet Security - http://www.ageuk.org.uk/Documents/EN-GB/Information-guides/AgeUKIL4_Internet_security_inf.pdf?dtrk=true

- Get Safe Online 'It's Always Personal' – video resource demonstrating the risks of using public WiFi and the prevention tips you should follow - https://vimeo.com/142180832