TECH ABUSE

Gender and IoT (G-IoT) Resource List

Leonie Tanczer, Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis

March 2019

This resource list is intended as supplementary material to better inform and guide victims and survivors of technology-facilitated abuse as well as those working with them.

It lists organisations which produce guidelines and advice, and highlights known methods of abuse which perpetrators may exploit. It also serves as a reference point to provide additional information on common cybersecurity and privacy issues.

The resource list has been developed by a socio-technical research team at University College London. The team's 'Gender and Internet of Things' (G-IoT) study was funded by the UCL Social Science Plus+ scheme, NEXTLEAP, UCL Public Policy, and the PETRAS IoT Research Hub. Research collaborators include the London VAWG Consortium, Privacy International, and PETRAS. The study examines the implications of 'Internet of Things (IoT) technologies such as 'smart' voice assistants or wearables on victims and survivors of domestic violence and abuse.

The list may be used together with our guide and policy leaflet which outline common IoT devices and their functionalities. These documents are all available on the Gender and IoT project website.

Please note, this document was written in March 2019. While we aim to update this document regularly and indicate changes through timestamps, hyperlinks and proposed recommendations may not always be accurate.

The resource list also does not replace advice from specialists, including the police.

While most resources in this guide are in English, we do highlight, when available, the existence of translations into other languages.

Should you have any suggested amendments, questions or concerns about the resource list, please contact the research team.

INTERNET OF THINGS-SPECIFIC ADVICE

Technology Safety is a blog managed by the Safety Net Project at the National Network to End Domestic Violence (NNEDV). The blog discusses technology, privacy, and safety in the context of intimate partner violence, sexual assault, and violence against women* and provides safety toolkits to aid victims. Most recently NNEDV published dedicated information to improve understanding of the use of IoT in domestic violence cases. Resources include information on how to spot and engage with personal assistants, connected health & medical devices, smart toys and location trackers. The resources are available both in English and Spanish.

https://www.techsafety.org/resources-survivors

Shodan

Shodan is a search engine where users can search for specific types of devices (including webcams, routers, servers) connected to the Internet using a variety of filters. It is best known for allowing users to search for vulnerable IoT systems, including smart video cameras or even traffic light controls. Device owners are frequently unaware that, for instance, their video recordings can be accessed through this page.

https://www.shodan.io/

eSafety Women is an online website produced by the Australian Government’s Office of the eSafety Commissioner. The website contains a lot of resources and has a useful interactive infographic to help familiarise the public with IoT systems which may pose a threat to victims in the home or a smart car. There are also downloadable guides with general information on tech abuse in 12 different languages.

https://www.esafety.gov.au/women

The Data Detox Kit contains tips to be safer online. It includes a section on IoT, namely on Alexa (the voice assistant in Amazon’s Echo speaker). There is also guidance on obtaining better control on what you share with the device, such as deleting recordings, muting the mic or using alternative services for Internet searches. The material is available in English, Spanish, German, French, and Portuguese.

https://datadetox.myshadow.org/en/bonus/iot

*Which also refers to gender non-conforming individuals.

DIGITAL SECURITY FOR WOMEN*

Tech vs Abuse is a collaborative research study about the use of digital tools to support people affected by domestic abuse. The project is supported by various institutions, including Comic Relief, Chayn, SafeLives, and Snook. The website points to ten initiatives by organisations such as Refuge or Rape Crisis Scotland, all of which aim to improve the safety of those affected by abuse and coercive control.

https://www.techvsabuse.info/

DIY Cybersecurity for Domestic Violence

This guide was developed by Hack Blossom, an activists and artists' platform concerned with digital rights. The guide includes threat scenarios and provides recommendations on how to resist a controlling partner.

https://hackblossom.org/domestic-violence/

Take Back the Tech is a global campaign that connects the issue of violence against women* with emerging technologies. The website offers safety roadmaps and information on cyber-stalking, hate speech and blackmail. The material is available in English, Spanish, and French.

https://www.takebackthetech.net/

Gender and Tech is a website by Tactical Tech that provides digital security trainings with a feminist perspective. The material is available in both English and Spanish.

https://gendersec.tacticaltech.org/wiki/index.php/Main_Page

Cyberwomen is a digital security curriculum with a gender perspective geared towards those who want to train others on digital security. The resource covers topics such as passwords, viruses and safe browsing. The material is available in English, Spanish, and Arabic.

https://iwpr.net/what-we-do/printed-materials/cyberwomen

SmartSafe is a website collating resources to support women* experiencing tech abuse. It includes videos, articles, and other formats covering technology safety.

https://www.smartsafe.org.au

XYZ is a space for practical tools to navigate digital security and privacy from a gender perspective. It is a space to learn from other women*, inspire one another and co-create. The page contains information on issues such as hate speech, useful apps, and online violence.

https://xyz.informationactivism.org/en/

Access Now's Digital Security Helpline

Access Now works with individuals and organisations around the world. They provide both advice on how to improve digital security practices as well as rapid-response emergency assistance. The 24/7 service is available in nine languages, including English, Spanish, French, German, Portuguese, Russian, Tagalog, Arabic, and Italian.

https://www.accessnow.org/help/

Coding Rights is an organisation ran by women* which highlights the power imbalances built into technology, particularly those related to gender. They have launched a collection of GIFs for women and non-binary people to increase awareness on digital security. These include advice on chat apps, secure passwords, safer nudes, and hate speech.

https://www.codingrights.org/safersisters-feminist-digital-security-hints-in-gifs/

Go Ask Rose is a group of security professionals working with victims of domestic violence and support services. Their website includes security guides covering topics such as social media, financial security, secure communication or disappearing online.

https://www.goaskrose.com/security-guides/

Empowering women to be safe online is a guide developed jointly by Women's Aid and Facebook. The document contains tips for using social media safely. It includes information on how to protect one's Facebook account and how to respond to abusive content.

https://fbnewsroomus.files.wordpress.com/2017/06/womensaidfacebooksafetyguide.pdf

DIGITAL SECURITY FOR CHILDREN

Thinkuknow produces online resources for children of different age ranges (5-7; 8-10; 11-13; 14+) as well as for parents/carers. It offers information on how to keep children safe online and links members of the public to the reporting function of the Child Exploitation and Online Protection Command, which is part of UK's National Crime Agency.

https://www.thinkuknow.co.uk

The **National Society for the Prevention of Cruelty to Children** (NSPCC) provides guidance about online safety for children. It explains how to set up parental controls, offers a helpline, and provides resources for parents, carers, schools, and teachers.

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

The **UK Safer Internet Centre** provides general advice for young people as well as specific guidance concerning the use of different social media platforms. The Centre offers a hotline for reporting and removing sexual images of children and offers training for a range of different audiences.

https://www.saferinternet.org.uk

Childnet offers resources for staying safe online, including guidance on cyberbullying, how to restrict in-app purchases, and how to set up family agreements to set clear expectations for a positive and safe Internet use.

https://www.childnet.com

Spyware

Online monitoring software such as **Spyzie** and **FlexiSPY** are frequently advertised as tracking software for parents/carers to monitor children's online behaviour. However, these programmes have been misused by perpetrators. These monitoring software packages have a wide range of capabilities, including setting a schedule to restrict phone usage, tracking a person using GPS or Wi-Fi hotspots, and accessing someone's messages, and browsing history.

End Tech Abuse across Generations (eTAG) is a project responding to the use and misuse of technology in sexual assault, stalking, and domestic violence cases, particularly among young people. eTAG provides a ‘Cyber Abuse Toolkit’ which includes tips to be safe online, and how to collect evidence of abuse. It includes advice for schools on dealing with online abuse. Most content is also available in Spanish.

http://www.endtechabuse.org/resources/

Stopsextortion is a website developed by Thorn, a non-profit organisation that aims to defend children from sexual abuse. The site provides resources for young people who may be experiencing ‘sextortion’- a type of blackmailing based on the threat of sharing private sexual information or images.

https://www.stopsextortion.com

FINAL POINTERS

The **CryptoParty** movement is a decentralized effort with community events happening all over the world. The goal of any CryptoParty event is to pass on knowledge about protecting yourself in the digital space. This includes encrypted communication, the prevention of tracking while browsing the web, and general security advice regarding computers and smartphones. These events are free of charge and are normally run by volunteers.

https://www.cryptoparty.in/

Cyber Aware is a UK-wide cross-government awareness and behaviour change campaign. It aims to drive behaviour change in individuals as well as small businesses, so that they adopt simple secure online behaviours to help protect themselves from cyber criminals and other malicious parties.

https://www.cyberaware.gov.uk/

The **Security Planner** by Citizen Lab is an easy-to-use guide with expert-reviewed advice for staying safer online. Users answer a few simple questions to get personalised online safety recommendations. An updated version of the Security Planner in languages other than English is expected to be released soon.

https://securityplanner.org/#/

The **CyberHygiene Insight Report** identifies what behaviours are currently expected of users of IoT products to properly secure their devices. It provides recommendations for the purchase, set-up, maintenance, and disposal of IoT systems.

https://iotuk.org.uk/wp-content/uploads/2018/01/PETRAS-IoTUK-Cyberhygiene-Insight-Report.pdf

The UK Government's **Code of Practice for Consumer Internet of Things (IoT) Security** offers guidance for manufacturers and relevant information for consumers of smart devices. The Code's 13 guidelines ensure that IoT products are secure by design and give pointers on necessary privacy and security features when purchasing smart systems.

https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security