We have quoted a lot of different research in episode one of Which? Investigates, so if you want to do any more reading here are the links to all the articles we came across while doing our investigation.

It's Tuesday, 20th September 20.16. News channels across the world are debating the upcoming US Presidential election, and in Washington, technology journalist Brian Krebs sits down for another day at the office. He logs into his blog, the incredibly popular "Krebs on Security" - and quickly realises something isn't... quite... right.
https://krebsonsecurity.com/

Almost a month later, October 20.16, and again without warning, there's another attack. This time it's not on Krebs, or any other individual person, it's on Dyn.com (pro.Dine), a company that - at the time - maintained data centres around the world - essentially huge banks of computers that keep the internet working. This attack is so successful that most of the East coast of the USA has problems with their internet connection and vital systems fall offline.
https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

What OR WHO caused such widespread internet havoc? A network of hackers in Russia? Or a terrorist cell waging cyber warfare? Nope. The whole thing was carried out by three college students sitting in their dorm rooms
https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

According to a 20.19 survey carried out by the Office for National Statistics the average UK household owns more than ten 'smart devices' - from smart TVs to smart doorbells to smart assistants that help do anything from turn the lights to open the front door, all by just using your voice!
https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/families/bulletins/familiesandhouseholds/2019#main-points

According to authors Lee Raine and Jemma Anderson- in their 20.17 paper 'The Internet of Things Connectivity Binge' - in 1999, 22 years ago, just 4% of the world's population was online
https://www.pewresearch.org/internet/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/

This scheme that Kate mentions will use sensors installed in people's homes to track behaviour and electricity usage with the aim of spotting any potential health problems and the technology company behind the research claim it could reduce the number of support visits patients need by 780 hours each year, leading to annual savings of around £250,000 in council spend.
https://www.bbc.co.uk/news/technology-58317106

In Season 1 of this podcast I mentioned the smart fish tank in the Las Vegas Casino aquarium that enabled it's owner to autonomously control the temperature of the tank, even feed the fish. However, it also enabled a clever hacker, 5 and a bit thousand miles away in Finland, to use the fish tank's internet connectivity to hack their way into the casino's network, stealing plenty of sensitive data...
https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Last year researchers from technology firm SEC Consult found that the private lives of at least 50,000 users had been exposed... by a sex toy! The, um, smart device could be remotely controlled via the internet from a mobile phone, and it was found to have multiple vulnerabilities which put at risk not only the privacy and data of its owners, but also their physical safety...

https://sec-consult.com/blog/detail/one-hack-of-a-valentine-when-iot-gets-under-your-skin/

Now, before you start getting too worried, the likelihood of someone hacking your baby monitor is distinctly small. If you do have one though and would like to know how to make it more secure we've got an article on the Which? website with an easy guide.

https://www.which.co.uk/reviews/baby-monitors/article/could-my-baby-monitor-get-hacked-a1JXu7s9CSYD

This is Kaushal Kafle, a PHD student at the College of William and Mary based in Williamsburg, Virginia. In 2018 he was one of the researchers involved in an often quoted piece of work that showed that hackers could use a smart lightbulb to gain access to someone's home.

https://qz.com/1493748/how-one-lightbulb-could-allow-hackers-to-burgle-your-home/

In 2018 the UK and US governments released a joint statement accusing Russia of state sponsored hacking on a global scale.

https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government

North Korea meanwhile is thought to have stolen billions of dollars in attacks in the last few years alone.

https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-arm

In their 2021 report, cybersecurity firm Crowdstrike even went so far as to say the number of attacks will only increase as the country [North Korea] reels from the impact of the Covid-19 pandemic.

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

It's called a Denial of Service, that's exactly what those students did on a big scale in 20.16 but there are lots of smaller examples, for example when hackers left the residents of two apartment buildings in Finland in the freezing cold for nearly a week by launching a denial of service attack on their thermostats.

https://thehackernews.com/2016/11/heating-system-hacked.html

The good news is that the government seem to be listening. In April they announced the snappily titled 'Product Security and Telecommunications Infrastructure Bill' which, when in place, will ensure companies do follow these demands.

https://www.which.co.uk/news/2021/04/smart-products-must-come-clean-on-security-under-new-laws/

According to Business Wire the global smart home market is showing no signs of slowing and it's predicted to reach a whopping 135 billion dollars a year by 2025

https://www.businesswire.com/news/home/20200724005173/en/135.3-Billion-Worldwide-Smart-Home-Industry-to-2025---Featuring-Schneider-Electric-United-Technologies-Amazon-Among-Others---ResearchAndMarkets.com