Being Hacked: Understanding Victims' Experiences of IoT Hacking

Asreen Rostami[12], Minna Vigren[2], Shahid Raza[1], Barry Brown[23]
[1]*RISE Research Institutes of Sweden,* [2]*Stockholm University*
[3]*Department of Computer Science, University of Copenhagen*
asreen.rostami@ri.se, minna.vigren@helsinki.fi, shahid.raza@ri.se, barry@di.ku.dk

Abstract

From light bulbs to smart locks, IoT is increasingly embedded into our homes and lives. This opens up new vulnerabilities as IoT devices can be hacked and manipulated to cause harm or discomfort. In this paper we document users' experiences of having their IoT systems hacked through 210 self-reports from Reddit, device support forums, and Amazon review pages. These reports and the discussion around them show how *uncertainty* is at the heart of 'being hacked'. Hacks are sometimes difficult to detect, and users can mistake unusual IoT behaviour as evidence of a hack, yet this can still cause considerable emotional hurt and harm. In discussion, we shift from seeing hacks as technical system failings to be repaired, to seeing them as sites for care and user support. Such a shift in perspective opens a new front in designing for hacking - not just prevention but alleviating harm.

1 Introduction

The threat of being hacked is sadly a common part of technology use. This is particularly challenging for the Internet of Things (IoT), since hacked IoT can be used to cause serious physical harm or discomfort, such as locking a user out of their home, or video recording their children. While much research has focused on the technical aspects of IoT security (e.g. [1, 42, 45, 91]), there has been recent interest in how users manage their IoT security (e.g. [5, 8, 62, 87]). Building on these works, in this paper we focus on the 'user experience' of being hacked: how users discover they are hacked, cope with the hack, and manage the damage done.

Our data comes from the discussions and reports from users who believe they have been hacked, posted on online discussion forums, product support forums, and product review pages. We focus on users' experiences of hacked IoT systems, since these systems both present particular issues in terms of user interface, but in the damage that a hacked device can inflict. From these online sources we collected 210 cases of users reporting having an IoT device hacked. These first-hand experiences and stories, and the online discussion around them, gives us new insights into these hard to reach experiences. Prevalent throughout this data was users' uncertainty and doubt around 'being hacked'. This is captured well by one poster who asked if his experiences were [a] "Ghost, cat or hack?" about their experiences. Users firstly asked *if* they have been hacked, then *who* has hacked them, and lastly *why* they have been hacked. There are also situations where users suspect they have been hacked, but are unsure if it is actually an intrusion, a technical problem or unusual system behaviour. For example, one common brand of smart home light bulb will flash on and off to indicate an error condition – and when this sort of behaviour happens across multiple devices, users reported confusion, concern and worry. These '*non-hack hacks*' are a major problem since users need to deal with them as if they are hacks, and so they can cause similar amounts of disruption, worry and personal pain.

In discussion we explore how this data lets us look at the social and psychological aspects of hacks. With a focus not on the hacks, but the people whom the hacks impact, how can we design for managing the impact that hacks have on users. We discuss '*cybernoia*' - where users become unsettled through a hack or suspected hack, but also how hacks can disrupt relationships and expectations around technology. This refocuses design attention from just preventing hacks to supporting victims, and designing systems that could take a support role similar to the roles the forums provide for users. In conclusion, we discuss how hacks interfere with relationships, in particular when the person who is behind the the hack is known by the victim.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

2 Related works

With our focus on hacking, users and IoT, we have drawn on two main research areas: first, research on user experiences of being hacked and second, security and privacy issues around domestic IoT. In addition, with our use of discussion forums as a source of data we provide a brief review of the use of online discussion data in HCI.

2.1 User experiences of being hacked

For as long as there have been computational systems, hackers have attempted to penetrate and hack these systems for nefarious reasons, and users of these systems have suffered from these attempts. Hackers' intentions and their experience of hacking have been a topic of interest in a number of different fields [19,38,44,80,90]. Research has also studied end-users' practice of hacking their own devices to make the device serve different purpose and interests, beyond the intention of the device manufacturer [11].

However, it has only been recently that the user's experience of being hacked - the victims' perspective - has come into focus. Tian et al. [79] document different types of cybersecurity incidents reported by users and describe victims coping mechanisms in dealing with these hacks. They in particular discuss how users felt ambiguous about some of these incidents, resulting in users denying the existence of the hack as a coping strategy. More broadly, this work has explored how victims of cybercrime [15,21,37] can be caught up in large-scale attacks on organisations [22]. This research also covers how a 'victim-blaming' discourse around online fraud as well as online humour and shame are used to push victims to stay silent. With the rise of online harassment [51,82], phishing [20,79,85,86] and ransomware attacks [14,71,73,89,92], many users and organisations have been targeted in hacks where they are faced to pay ransom money or experience devastating damage to their digital ownership of their properties and data. In one example, Zhao et al. [93] studied a group of attending surgeons' experience of a ransomware attack that caused the shutdown of their hospital. Their study demonstrates how such incidents caused not only disruptions in their online communication but also affected their process of carrying out of surgery and medical procedures.

One area of growing concern is technology-mediated abuse, where hacking or technology is misused as part of violence between current (or former) partners. Parkin et al. [62] document a number of different types of threats where, for example, a security camera can be used (hacked or otherwise) to facilitate intimate partner abuse. Bellini et al. [7] take a different research angle, and present how potential perpetrators use online resources to plan, discuss and legitimise their use of technology in intimate partner abuse. In a related study, Freed et al. [30] discuss how in intimate partner abuse, the attacks performed by the abuser are not necessarily technologically sophisticated, rather the abuser uses their knowledge about the victim to crack passwords and hack into their accounts and devices. One concerning issue brought up in this study is how victims cannot always remove a compromised device from their network, since that device is used by the victim to gain access to professional and social support to deal with the hack. Removing the technology might solve the problem, but could put the victim in danger of isolation [31].

For this study, we were specifically interested in IoT hacks, in part because these systems present more constrained security user interfaces to users, but also for the ways in which IoT hacks risk a potentially higher level of material harm for users. As Slupska points out, consumer IoT products while marketed to support protection and care actually create new vulnerabilities - particularly with respect to domestic violence, something almost entirely ignored in the smart home security analysis literature [74]. Mckay and Miller [58] discuss how home IoT devices can be used to perpetuate new forms of harassment and coercive control in the home environment, moving beyond hacking into 'traditional' technologies such as mobile phones or personal computers. Levy and Schneier [52] broaden this discussion by highlighting how within intimate relationships privacy and security threats can arise from the lack of appropriate design, and how cybersecurity broadly ignores the different data sensitivities that can occur within relationships. This has resulted in systems that do not protect against intimate threats [53]. The relevant and timely concerns expressed in these studies open up the study of user experiences of IoT device hacking.

2.2 Security and IoT

HCI (and related work in UbiComp) has developed an extensive body of work around the user experience of IoT and home IoT in particular [8,16,26,32,39]. HCI research have increasingly brought more privacy relevant research to the fore [31,48,64,65], and called for revisiting users' privacy design with respect to vulnerable populations (e.g. [57]). In one study, Choe et al. [18] studied privacy in relation to parents' use of smart security cameras at home as part of a 'responsible parenting' strategy. In a related study, Worthy et al. [88] found that users of IoT devices are often concerned about the trustworthiness of the device, particularly in terms of the data it collects as well as the person or organisation who controls the functionality of the device. In another study, Bouwmeester et al. [8] present different steps that a home IoT user may take to identify a device infected by malware. Their study highlights how participants felt uncertain about whether they have correctly identified the infected device, and how some participants failed to fully execute the recommended actions to remediate the infected device due to design complications or simply because of lack of security knowledge and experience.

In a series of original papers, Pierce [64] uses the 'creepiness' of internet-connected security cameras in domestic contexts to discuss hole-and-corner applications that make use of user data out of the context of the service they should provide, in a hidden way that could harm the user. For instance, neighbours could misuse security cameras to monitor others' religious commitment to digitally gaslight and blackmail them. Other scholars have also studied how users of IoT devices perceive the security and privacy of their data being used by these devices [43, 78, 94]. For instance, Jacobsson et al. [43] highlight the importance of understanding user interaction with IoT devices "in order to create usable privacy mechanisms". In a similar vein, Zheng et al. [94] studied how users perceive privacy when using IoT and what are the different approaches they take to protect the privacy of themselves and their homes. Their study highlights that the majority of users put their trust in the hand of the well-established brands and manufacturers to protect their data and privacy, selecting the device based on the vendor's reputation as well as online reviews about the device. One interesting aspect of this study is that users of these devices have reported government and Internet Service Providers (ISP) as the most worrisome outsider actors from which they wish to protect their data, rather than hackers. At times, this perspective served, perhaps, in light of the recent critical debate on state surveillance [72] and the commodification of personal data. However, during recent years and with the increased popularity of home IoT devices in the consumer market, home IoT users have witnessed and dealt with threats and security intrusions committed by different groups of individuals. Reports on various network-connected devices being exploited by criminals and hackers, such as baby monitors [3, 83] and smart doorbells [23, 63] are few examples of these security threats posed by different groups of bad actors with different goals and agenda in mind.

2.3 Forum Studies in HCI

The main data source we use in this paper comes from forum data posted on the internet. HCI researchers have broadly used online communities and forums as part of understanding both internet behaviour and community structure [55, 70] but also more generally to investigate users' motivations for their participation in online forums and communities [47]. Collecting data from users participating in different online communities and forums have been a rich source of data and inspiration for both HCI and CSCW communities [17, 27, 33, 46, 61, 67]. Particularly in the domain of health, research has looked at how individuals adopt or disengage with online communities [56], how these forums are used by patients for recovery [54], and how patients share their knowledge and experience of the medical condition to support each other [41, 67] as well as discussing the potential challenges for clinicians to participate in these forums [40]. Previous research [28] has also discussed the ethics of using online data for research, by presenting how users of online communities, such as Twitter, can have different attitudes toward privacy, and their expectations can be highly context-dependent. In their studies, Fiesler et al. [28] & Bruckman et al. [13] suggest that researchers should take extra measures to minimise potential harms that could arise from neglecting the privacy of online users by, for example, careful anonymization of names while making sure that the published data is not linked back to the online original account.

Forum studies are effective at overcoming methodological challenges such as collecting data from communities who are isolated due to social and geographical constraints. Moreover, collecting interview data when participants need to disclose sensitive information about themselves or their experience (such as understanding survivors of sexual abuse [4]) has proven to be a challenging task, as many survivors wish to remain anonymous or find it hard to talk about their experience outside the social media context due to their traumatic experience. Previous research has also discussed how the rarity of cases as well as the stigma around speaking about the topic have affected the research and data collection strategy. Such a case can be seen in identifying early adopters and early victims of a particular technology, for example in studying victims' experience of technology-mediated abuse [58]. Research have also reflected on the difficulties of collecting interview data from participants around a phenomena due to an ongoing world crisis such as outbreaks or pandemic. For instance, Gui et al. [34] use online communities to collect data from geographically distributed travellers affected by the Zika outbreak, something that could not be collected directly due to resulting travel restrictions.

3 Methods

For this study, we were interested in understanding better the experience of hacking victims, how they make sense of the hack, and in particular the different practical and emotional resources they deploy to deal with being hacked. In planning our data collection, we were concerned that the social stigma attached to being a victim [4, 22] could affect the quality of collected data, and that interview data might be unreliable as in cases where there is a strong social desirability bias [10]. Moreover, during our initial attempts to recruit interview participants we found considerable hesitancy to talk to researchers about these sensitive issues. This led us to explore other means to collect data. Looking online for users' reports of being hacked, we were surprised to find many reports in general online discussion forums (Reddit), product support forums, and user-generated product reviews (Amazon). There were also extensive responses and discussion of the initial posts – spanning from related stories, advice around dealing with and repelling attacks, as well as broader discussion around the hack, the hacked devices, and IoT security. This led us to explore how online posts could be used as a data source.

As we discussed above, forum data has been used in user research, often as part of investigating sensitive topics. These explorations usually take a dual path – first, the forums themselves are a topic of study, the types of contributions and how the forums benefit those who contribute or read posts. Second, the actual content on the forums provides an insight into users' experiences outwith the online forums. Internet posts have a number of advantages over reports collected through interviews. Interviews as a method shape and prompt data in strong ways by the questions being asked, and the responses of the researchers [6]. Forum posts offer the advantage of being naturally produced data, as well as containing responses of other posters. This said, the lack of control over the data does mean that it is harder to check and validate data. Participating in an online community is essential so as to learn possible in jokes, 'house style' and the like that might mislead a researcher or 'outside' readers of the forum content. It is also important to maintain some scepticism around posts and responses and recognise that trolling is a common aspect of all online interaction.

We collected our data during January - March 2021. Before conducting our study we informally read and participated in Reddit forums around IoT device support, smart homes, cybersecurity, and hacking. Building on this we searched media coverage and security reports on vulnerabilities on IoT devices. Through this pre-screening of vulnerable devices, we were able to identify a list of 13 hacked devices from different brands that served as our seed list of devices to look for stories from users from online forums. These devices included security cameras, smart locks, doorbells, lights, TVs, speakers, and voice assistants. We used the forums' internal search function and applied the brand names, general devices names, as well as keywords such as *smart home*, *home IoT* in combination with*hack* and *hacked* (Appendix A: Table 1). This actual data collection expanded the list of devices as the searches from these forums brought up new devices to be included in our list of hacked devices (Appendix B: Table 2). From this, we collected together a corpus of 210 hack reports and posts along with the related discussion. From Reddit we took data from subreddits with 114 posts (54% of all the data), product support forums with 84 posts (40%), and 12 Amazon reviews and product support forums discussing being hacked (6%). Overall this was more than 1000 pages of data.

It is worth mentioning that while our focus was on collecting reports of hacked IoT devices, we found that often reports of security vulnerabilities for these devices would come not from the devices themselves but from the WiFi network they were on, or the management account with the company that made the device. This meant that our data includes reports that were somewhat associated with an IoT device (as reported by the original poster), such as routers and the network where the device was installed. One motivation behind this data collection decision was – as we shall see in the analysis section – while the devices themselves could be hacked in various ways, a home IoT device exists in a complex network of other vulnerable access points. Indeed, access to the home WiFi seemed a common vulnerability here, since home WiFi passwords are often rather weak and shared relatively broadly within the household members and even with guests. Being on the same network, therefore, could be used as a way of accessing IoT devices, sometimes without any further security needed. WiFi speakers, and TV video streamers, are a few examples that could then be vulnerable to unwanted access.

We analysed the data set using an open coding method. Our coding process was done using NVivo. Independently, two of the authors coded 50 threads each and developed their own codebook [49]. The research team then met, discussed this data and codebook, and in discussion formed a joint codebook. A small number of threads (5) were coded together in this joint session to test the joint codebook. Each author then coded the rest of their own data sets independently. During this part of coding, new codes did arise along with refinements on the old codes, which were addressed in two further joint sessions during the coding process. The final codebook (Appendix B: Table 3) included 32 main codes that we used to organise our data. These codes were aimed at categorising our data based on, for example, the type of the device, the description of the incident or hack, the (presumed) motivation behind the incident, the identified actor(s) behind the incident, the evidence available or shared about the incident, discussions on the analysis of the (presumed) hack, harms and damages caused by the incident, actions taken by the OP, and their existing security practices.

This categorisation helped us to analyse the whole corpus in a systematic manner, further identify patterns and develop themes through an in-depth iterative and collaborative analysis process. The categorised and coded data were then iteratively analysed using thematic analysis [9]. In doing so, we mapped our data to the themes that we had identified contributing to developing an understanding of how and why users share their stories of being hacked in online forums, what the different types of online interaction they engaged in during this process are, what type of hacks they have encountered and dealt with, what kind of collective sense-making is entailed around different shared cases, and what (if any) the consequences of the incident were.

3.1 Ethics

We have restricted our data collection to those forums that are available to the public without the need for registration and considered these forums as public material [77]. However, we have not collected any personal data about the users of those communities that we studied beyond their reports and posts and content provided. In presenting quotes in the results sections we have provided most quotes verbatim, resonating with Brown et al. [12] argument that anonymity should be provided when "participants *want* to be anonymous.". However, to ensure the safety and anonymity of those who have experienced serious threats, report serious mental health issues, or accuse an individual of wrongdoing, we have paraphrased our quotes in a way that it is not easily traceable to the Original Poster (OP) and the community they were engaged with [25, 66]. In doing so, we have kept the core concerns that are mentioned in posts and the type of device they have used but removed the brand and name of the specific forum they have originally posted.

4 Results

Our analysis is broken into three sections. We start by discussing how users reported being hacked on the different type of online forums we studied, and in particular how users report their hack experiences. Second, we discuss how users dealt with uncertainties around being hacked, and the doubts they have about if, how, and who had hacked them. Lastly, we discuss how users deal with hacks, and the lengths to which they go to understand the hack and to deal with the hurt and harm it causes.

4.1 How users report being hacked

The posts we analysed spanned from users asking the simple question "Was I hacked?" to much more detailed descriptions of events, technology in use, actions taken to solve the situation, evidence to back up the incident, and social dynamics that have caused the situation (as in the case of (ex-)partner abuse or neighbour harassment). These hack descriptions give us access to users' accounts of what it is like to be hacked, but also how users detect hacks in the first place, how they identify the nature of the hack and its potential source, as well as how they attempt to 'fix' the hack, and deal with the problems that the hack causes.

A prevalent feature across all our data is the way in which users tell their 'hack story'. End-users recount 'what happened' by telling the general story of how they discovered the hack, the evidence of what makes them think it is a hack, and how they proceeded to deal with the impact of the hack. As an 'exceptional event', users often go to great lengths to explain why they suspect a hack, rather than more benign explanations. As is typical when individuals describe unusual events, the justification of an unusual event is preceded by evidence that shows how more mundane explanations could not apply [68]. As we quoted in the introduction, a user asked the question 'cat, ghost or hack?' in the title of their post – if it is not an accident (the cat), or the paranormal (the ghost), this it must be - as a last resort – a hack.

Post were sometimes met with scepticism as to the reliability of the story, or the 's motives. However, more commonly those who responded took the stories seriously, offering a range of helpful responses, spanning across technical, social and practical support of different sorts. As with storytelling more broadly [69], these 'hacked stories' often prompt the telling of follow up 'hack stories' by other posters. These first stories thus prompt 'second stories' of similar hacks that had happened to other users, either with the similar technology or similar in form. In the Reddit and product support forums, these second stories would take the form of follow-up posts sharing a poster's own story. Elements of the hack then would be taken apart - discussed for their relevance in different ways. Interestingly, even with the online reviews - although the format does not lend itself to responses - reviewers would start their own reviews by referencing earlier reviewers, such as "*I also had my security camera hacked*". Reviewers then would connect together reviews to provide cross-validation of experiences and give added credence to the warnings of vulnerable technology. Besides asking for help, these second stories are often rich in content including also warnings about the product, discussion on cybersecurity in general, complaining about bad product support and design, or admonishing the manufacturer for a faulty product.

Looking over the corpus, we can characterise three elements that reoccur in the hack posts: *warnings*: descriptions of problems with, and a warning against buying a particular device, *calls for support and help*: where a post asks directly for support with dealing with the hack, and *initiating discussion*: more conversational points where the aim seems to be more to start discussion around the hacking incident.

4.1.1 Warnings

Some parts of posts are written essentially as warnings, with a user reporting their hack as evidence of the unsuitability of an IoT device. For example:

"It was the best camera till it was compromised. I got it so I could make sure my place was secure. BUT sure enough last night [...] at about 9pm [...] I WATCHED IT MOVE 5 DEGREES TO THE LEFT [A]ND THEN BACK TO THE RIGHT! [...] I strongly urge you not to buy this camera because if one is compromised then most likely their system is too".

Warnings were most common in the product reviews, although they were not unique to the reviews. In some posts, the reported incident was only briefly described, with the description rather focused on pointing towards describing vulnerabilities in the device, and the user offering a brief recount of the experience of the hack or problem. With warning posts, the original poster is 'making a case' about the device, justifying their warning by referencing their own experiences, others' experiences, and even in some cases media reports or other online discussions.

4.1.2 Calls for support and help

A second element was the more direct asking for support, either from other users or directly from the manufacturer. These requests spanned questions on how to protect oneself against the (presumed) hack, but in more desperate cases, they were pleas for help to know what to do next from exasperated users who had no idea what to do and what was going on. For instance, in the following example on the Chromecast support forum, a user reported about their hacked device, asking for help not only from the community members but the Google product team, while also reporting on their immediate action to call the law enforcement:

"My Chromecast was hacked and turns my tv on with creepy short videoclips.. what is going on? [...]. I called the police and the Az Attorney Generals offic".

While manufacturers do respond, they usually answer through a template of asking for particular information. So, for example, with remote cameras there is usually an attempt to obtain a copy of access logs of some sort through which the manufacturer can detect who had accessed the data and whether the incident is in fact due to unauthorised access or something else. Follow-up posts by others often offer stories of earlier reports, and earlier solutions provided by the support team, demonstrating similarities in hacks across the life-cycle of the product. Interestingly, these requests for help are not always technical in nature. Especially in the case of 'known hacker hacks', the requests for support and help can be more emotional and practical in nature, such as who to report a hack to, or how to deal with the relationship with the hacker.

4.1.3 Initiating discussion

A third element of the post was when posters gave more detailed descriptions of the hack, where the intention of the OP seems to be more to initiate discussion and hear if others have experienced the same. In these posts, the shared story can be seen as reporting the hack as part of asking for advice and opinions from others but more importantly as an opening for discussion. As in the following quote, the OP describes what has happened and the actions they are planning to take like contacting the manufacturer, with the ending question on wanting to know if anything similar has happened to others.

"10 minutes ago my Arlo camera in the kitchen started making pornography sounds through it speaker, it lasted around 30 seconds. Just before the event my google home speaker made the blimp noise as if someone had said the trigger words. My Arlo is linked to my Smarter things hub, google home and I think the ifttt [if this then that] service. I guessing something has been hacked! This is not a joke and is freaking me out. During the sounds the lights was on as if someone was watching. As you can imagine I have turn everything off and will be contacting Arlo support to shed light on the event. Did anyone else experience thus, surly I wasn't the only one".

Posts like these would usually be responded to by follow up posts from other users which replied to the concern over IoT security and discussed different aspects of it but also provided practical security information – such as protecting and changing passwords, or setting up two-factor authentication (2FA). The example above received 20 replies from 15 Reddit users. These responses include broad security advice that describes how to 'delete and wipe' a network that has been compromised and ways of re-securing home technology in such a way that it would not be vulnerable to being hacked all over again. This discussion takes a number of different directions but responds to the different issues raised by the original post - the different services outlined, the hack and whether it did take place and so on.

4.2 Making sense of the hack

We move on to consider perhaps the core problem that our posts reported in dealing with hacks - the problem of knowing what is going on and how to deal with uncertainties around hacks.

In the posts, we analysed it is the users themselves who define their own experiences as 'being hacked' and choose to post or respond to others' posts. This means that we are including many cases that would perhaps not fit with security professionals' definition of being hacked, or even a common sense understanding of a hack. Uncertainty about the status of a hack is ever-present in our data, and this leads to the issue of how 'uncertain' hacks should be approached since they often still can cause real hurt and damage. In some cases, it becomes clear through the online discussion that the OP themselves are actually mistaken about the hack, and that it is some sort of other technical problem in the functioning of the IoT device. We characterised these cases as 'non-hack hacks', in that even though the OP is mistaken, and the hack did not actually occur, the 'hack' has a real harmful impact, described by the OP in terms of the time they waste to diagnose what has happened, the worry they have around the hack and the emotion cost of originally believing they were hacked.

In some threads, the OP later reveals that they were joking, a trick was played on them or that the post is not to be taken at face value. Clearly, paying attention to the discussion alongside the original post is important here. By analysing forum data, we have the advantage of having responses from others and follow up posts from the OP which can shed light on the original story, or at least put it into some context.

Indeed, uncertainty was a prevalent feature of users' hack experiences - uncertainty about whether they had been hacked, uncertainty about who might have hacked them, and uncertainty about what to do about the hack. Users start by being suspicious about something that has happened with their IoT system - this might take the form of unexpected system behaviour – such as an IoT light flashing on and off without user intervention or a security camera moving or making clicking sounds. Depending on their technical skills or experience, the user usually collects 'evidence' about the hack, trying to find out if they have been hacked by looking at the system behaviour, checking security settings and logs in order to make sense of the incident or to investigate what is going on. In the cases we analysed, this often leads to some attempt to fix the problem – to repel the hacker or to find some way of barring entry by the hacker (such as changing a password or turning a device off).

4.2.1 Have I been hacked?

As we described above, the hacked stories often contain a 'cry for help' of sorts, with OPs using the platforms with the hope of receiving an outsider' perspective to help them make sense of the incident and better understand it. Indeed, to a non-expert user, nearly any unfamiliar or unexpected behaviour can be seen as a suspicious action or a potential hacking alert that they need to deal with. For instance, a post to Reddit describes an unexpected action occurring without a chance to verify if this is a hacking attempt:

"Is my Alexa Hacked? I have recently put an IP camera to monitor my cats activity while I'm sleeping and away [...]. A couple days ago I was reviewing the videos [...]. At 3:20am (halfway through the video) you can see the light on the Echo Dot go on. It stays on for about a minute. Nothing is said or heard except for silence. When I checked the history in the Alexa app there is absolutely nothing that triggered it to go on. There have been a few times when Alexa has started recording without being prompted but I can usually listen to what it was...this was just completely undocumented. I cant find any logs on how to check what prompted it to turn on. It's been bothering me ever since".

In response to this post, posters discussed the different scenarios that could be the reason behind the system's behaviour. For example, one poster highlighted how this could be a less-known feature of the device, designed to communicate some system changes, particularly "*when software updates are applied*". So while in this case, it is perhaps unlikely that the Alexa was hacked, the user has been "bothered", to the extent of posting on the forum for help. This uncertainty does not always stem from a lack of technical knowledge - it can also comes from the complex and ambiguous design of particular IoT systems. Without any screen to explain its behaviour, for unobtrusive alerts the Alexa can only turn its light on. The device does not give any additional explanatory feedback about ongoing background activities (such as system updates), or how the device's visible features (such as lights) react or change in response to these activities.

Indeed, the most common question posted to the forums was in varying ways asking "have I been hacked?". The forums have many cases where users encountered an incident, which they think might be a potential intrusion, but were unsure how this could have happened, and wanting to know if the device is 'hackable'. In one example, a user recounts their experience of hearing a whisper coming from their security camera but being unsure if the device could be exploited by a hacker:

"I'm no tech-savvy over here, but I need to understand logically if there is a possibility that the Yi Home Camera we are using is being hacked. Last night we decided to move the camera from the living room where my son plays to the bedroom and a couple of minutes later while putting him in bed I heard a very clear whisper of someone saying something. My husband thinks I'm hallucinating (I'm sick with a bad cold and been taking Advil from the fever) but I swear I heard a voice from the camera. Can someone tell me what to do and if we should worry, or if this is just simply nothing? I've disconnected and deleted the camera".

This process of doubt and uncertainty can be quite harmful – with some users go as far as to questioning their mental health, or having their senses questioned as in the quote above. In one post to Reddit about a similar incident related to a different device (a Ring doorbell), the OP questions their mental health and suggests that another explanation to the scary event could be paranormal activity:

"So last night I had the most paranormal experience of my life. My wife had just gone to bed, I was the only person awake in my living room. I was playing a game on my iPad and had just clicked on a Netflix show. It got stuck loading at 25%. I wasn't paying much attention to it, it was completely silent and I hear someone whisper "hey guuyyssss.... heeeeyyyyyyy". I immediately grab my gun and clear my house. All my windows are shut, no one is around. The voice came from inside my living room. I then remembered my ring was charging, but I have 2 factor authentication, so I would know if anyone tried to log in or attempt to change password. My wife was passed out, and it was 100% a male voice. The only solution I have to this is someone has access to my ring and was playing around. Is this a common thing? Because it scared the living shit out of me and I still have no idea where it came from. Either I'm going crazy, there's a ghost in my house or someone got into my ring account".

Mental health state, or relating the incident to something paranormal, is in fact a common thread in our data, and mentioned by OPs or their family members as well as suggested as an explanation by other posters as well. In further discussing the previously quoted incident, one user contributes to the discussion of possible scenarios of occurrence by suggesting the OP may suffer from a momentary 'auditory hallucination' implying that the hack could not have happened perhaps because of the lack of evidence of intrusion or technical possibilities of performing such a hack with 2FA being in use. This shows that the likelihood of hacks is still considered rather exceptional, even though in this case there are reports and verified cases of similar incidents in relation to this specific device: *"Are you on any medications? Auditory hallucinations are a thing that can randomly happen with or without being on medications. It doesn't necessarily indicate a bigger issue. If similar things recur I'd look into getting medical advice though".*

4.2.2 Who hacked me?

Once the user suspects a hack has taken place, attention then moves to other aspects of the potential hack. One key question is *who* might have hacked the user, and in particular if the hack is from someone known or unknown. Most frequently the hacker was identified as an unknown person – as 'someone':

"I think someone has hacked my smart TV. So I'm sitting down playing Minecraft and all [t]he sudden my screen goes black for a few seconds my TV then automatically switches into screen cast mode and porn begins to play I don't think anyone's in cast range".

Although in many of the cases, the possible hacker remains unknown, it is interesting how common place it is for the OP to suspect a close person being behind the hack is. In these cases, the posters can go through in detail candidates for the hacker, for example, (ex)partner and neighbour, discussing if they have a vindictive goal and agenda. In the following post, the OP describes how they think that their security camera's unexpected behaviour is the result of their ex-partner having possibly hacked into their network and the camera, trying to abuse and stalk them in their home. They go on to describe how their camera behaves out of control, for example, by keep changing between the day and night mode even though their room with the camera is "bright enough, and not dark all.":

"Because I have a stalker, I purchased and installed a security camera. I am terrified [...], and needed some sort of security. It could be other individuals too, but I think it is my ex-partner and it is him who is messing with my life. [...] I think he is monitoring me on a camera and he has hacked our network... he tells our kids about what we have done at home. He moves thing around so I can realise he can come and do these things. I have installed the camera so it faces the door and records those who enter. It send me a notification if any movement happens. Then the other night I got a notification on my phone because camera shifted between the night and day mode over and over, and the blue frame in the app showed it is trying to detect something, but it couldn't. Our room was bright enough and not dark at all. I want to check with you folks here, is it possible to hack this security camera?".

While the OP here is trying to understand whether such a hack is possible from technical perspective, they also highlight a cause and effect relationship between their abusive ex-partner and the ongoing "odd happenings". From their point of view the ongoing abuse and previously documented and reported harassment of their stalker ex-partner are good enough reasons, and a catalyst, to believe it is them behind the incident while also being open to the idea of the incident could be done by "other individuals" as well.

In a related way, neighbours or friends were also often suspected as being behind hacks, building on existing bad relationships. The following example is taken from a post in a community forum of a brand of security camera, where a user reports on how they think one of their neighbour is hacking into their smart camera, perhaps because of their previous ill-mannered actions towards the OP or their suspicious actions around their property:

"I have more than two of this type of security camera and I have used them for some time now [...] Recently there were some problems and I assumed that the issues I was experiencing with my cameras were related to the updates. I now have a strong suspicion that my neighbour has hacked my accounts. I have already set 2FA and changed passwords couple of times [...] Some illegal activities have occurred that resulted in property damages and somehow that period of time is not recorded.".

4.2.3 Why was I hacked?

Another central aspect to these reported incidents is the collective sense-making around the motivation behind the hack. As described earlier, for those cases where OP themselves could identify the hacker, or be suspicious of someone, the motivation seemed to be more personal and easier to speculate. For instance, one person reported they think their device or network is being hacked because their neighbour "dislikes" them or the hack is a form of revenge and the result of dispute over statutory nuisance:

"I am in a noise battle, playing loud music and all of that, with my neighbour downstairs. They started all of this and now they have hacked my computer or wifi. I know I am hacked because they have sent me an email to me from my my account".

Previous HCI research [30] have already reported on several cases from which smart technologies at home being exploited by intimate partners to not only invade the privacy of the victim but to abuse them physically and psychologically. As in the example from the ex-partner's assumed hacking described above, the intention of the hacker was identified as to scare them, to monitor and control their life or as they put "to mess with their life".

Another set of cases in which the motivation of the hack was discussed among community members are those that OP could not identify any personal relationship with the hacker. What seems to be a common acceptance among this group of community members, including victims of these hacks, is the fact that many IoT users may suffer from data breach and hacks, simply because users tend to re-use old passwords for their accounts which can result in their credentials being exposed and exploited by 'bored teenagers' as one user put it: "*It sounds like bored teenagers who found some credential dumps, and started trying them against Ring until they found a victim*". For this group of users, the incident is not seen as a threat targeted towards them, rather they are most likely victims of opportunistic exploitation of technology vulnerabilities. As one Reddit poster describes "almost certainly [they] were not specifically targeted. The slim minority of people who get targeted are either political targets, or known financial targets, or being stalked by people they already know.". Such a perspective, can be seen in relation to several reported hacks and incidents associated with famous mass incidents such as hacks of Google devices (e.g. smart speaker, Chromecast) or Ring security camera and door bell:

"Every 20 minutes or so my TV switches to some crappy YouTube video about PewDiePie with shitty rap music and a "#ChromecastHack" hashtag. Anyone know how to stop this, it's driving me bonkers".

The "PewDiePie hack" originated from a YouTube subscriber battle between different internet channels, with hacks of printers and video players (such as the Chromecast). In this example, reported in Reddit, the OP and other community members affected by the similar attack discuss different motivations for the hack. What is central to their discussion is that hackers, whether they are PewDiePie fans or not, have not targeted a particular individual and do not seem to have vendetta towards a specific group of users. Rather it is a mass exploitation of existing 'feature' in the router, namely Universal Plug and Play (UPnP) to raise attention and awareness about an identified vulnerability in UPnP. This has also been seen as a way for hackers to simply show off and 'boast' about their discovery and hacking skills, or bring attention to a specific YouTube channel. In our data, we have also similar discussions in relation to a series of a controversial printer hacks by TheHackerGiraffe. In this hack the motivation was described by the hacker[1] and part of the community as a way to get the public's attention to an existing vulnerability in network printer that allowed anyone outside the network access a users printer. In this specific case, the hacker was seen both as a 'bad actor' and a 'concerned citizen' by "drawing attention to a real issue in a fairly harmless way. There is a security issue here and it should be fixed.", as one Reddit member put it.

In contrast to the examples documented above, we learned about cases in which the device owner misread the situation by assuming the hacking incident is a prank played on them by those whom they have shared the device with– or pranks that they took as evidence as they are being hacked. One common functionality that was being used and manipulated in these incidents is the two-way talking feature of the device (e.g. security camera or door bell) that allows the hacker-prankster speak with the people in the vicinity through the device's microphone. While this feature is mainly available to the trusted individuals who have access to the device or the related app, there are ways to gain such access through exploiting vulnerabilities available in the network or the accounts connected to the app and device:

"My wyze cam pan was sitting next to me. Motion detection and the pan setting off. It was facing 45 deg from me. Suddenly I heard the speaker come on and the camera begin to rotate around. It faced me and looked back and forth between me and my dog. I would say it was just resetting or panning, but the speaker came on like someone was talking through it".

In this case, while community members are sharing similar incidents and suggesting solution, OP further provides an update saying that the hack was in fact an innocent prank: "*UPDATE: LOL MY GIRLFRIEND WAS FUCKING WITH ME. MY BAD FAM*".

Although this case turns out without any reported harm, we learned of cases where the situation was initially perceived as a joke or a prank and then it was realised as a hack. In one example of this type, the OP has initially assumed the security camera incident is a prank played by their partner, the only person who has access to the device:

"Someone hacked my ring indoor camera by screaming to try to scare me and I thought it was my boyfriend who is the only one who has access to my camera. I immediately called my bf to ask if it was some kind of joke and while I was on the phone with him they were taunting me and my bf could hear them [...] They wanted to negotiate something with me and tried telling me to hang up the phone and that it wasn't my boyfriend. I'm shaken and called 911 and the city police to file a report. I'm actually on the phone with Ring to see what happened".

This OP later returned with an update about the incident after discussing it with the device manufacturer's support team. While we do not get the full details of the event, we learn that the technology has been (mis)used by the hackers to gather information or compromising material on the OP to blackmail them:

"*Turns out someone from the dark web stole my info. they tried getting money out of me by "negotiating" and then threatening me.*".

4.3 Dealing with the hack

Discussions of how to deal with the hack and finding a temporary or permanent solution for the problem is another characteristics of users' posts. Similar to the collective efforts in making sense of the hack – who, how and whys – community members shared their own practices as well as their successful or failed stories and solutions. This sharing often vary from technical advice on how to 'patch' the problem by resetting the password associated with the device, to a more practical conversation on how to report and deal with the situation, or how to emotionally deal with being a hack victim.

4.3.1 Getting technical support

Apart from technical advice, such as password reset, many community members provided information and advice on how to increase security measures by setting up a two-factor authentication, as well as a more educational content on how to identify similar security vulnerabilities in other devices or in their network in order to prevent future similar incidents. For instance, in one case the OP discussed how occasionally

[1] https://darknetdiaries.com/transcript/31/

their TV would turn on in the middle of the night without their permission. In response, one user suggested to start with changing their WiFi password in a more detailed manner, helping the OP to find their way in dealing technical difficulties of such a task, going through how to change the WiFi password, and how to check on the type of wireless encryption that was enabled.

One point to make here is related to the level of technical knowledge one needs in order to deal with 'basic' security functions in different devices. While users may be become accustomed to the basic requirements of keeping the device working in their domestic environment, for casual and non-technical users the topic of security can be overwhelmingly technical. The complexity of these connected devices has created complex requirements user, making them security-dependent on others [24, 36] or in this case online strangers who can help them understand 'what is going on' and what they should do.

4.3.2 Getting social and legal support

Alongside the technical support given in response, there was also often a practical discussion of who the OP could go to get help from others. This could span across law enforcement and the government (such as security agencies), and more prosaically help from the manufacturer. Indeed, in a few cases OPs themselves have mentioned contacting the police department as a practical legal and security practice in order to investigate the case.

The majority of advice for contacting the law enforcement came from community members, particularly in relation to those cases in which the attack required professional and technical attention related to an ongoing harassment. This also included those cases where children were affected or OP's life and safety could be in danger. While for many users, reaching out to law enforcement agencies was seen as a legal action towards solving the problem or preventing the victim from further harm, there was also considerable suspicion about whether ordinary law enforcement would have any understanding of technical issues. Rather, the expectation was that law enforcement's response could be used to give a warning to those, or a 'fright' to the likely perpetrators of a hack:

"You can try and call the police and show them evidence of your WiFi being duplicated and showing them the MAC addresses of the devices connecting to your wifi access point. There's a good chance they'll just have a talk with your neighbours but that might make them shit their pants enough that they stop".

4.3.3 Dealing with harm and hurt

Several users reported the financial loss associated with purchasing a device that was now useless due to a decision to uninstall the device and replacing it with a trustable device after the incident. But perhaps the biggest harm came from *emotional* burden of being hacked. Many users who experienced their IoT device being hacked, reported on different range of feelings, from being uncomfortable in having the technology at their home after the hack, to being scared of the 'spookiness' of the technology failures, to having a mixed feelings of confusion, anger, and worry that comes from not knowing for certain whether they have been hacked or not.

Perhaps the most devastating feeling reported comes from being unsure if the device is hacked or is being used by someone whom the users trust to share the device with, in a way that we do not understand. Many of the home IoT devices the users discussed were acquired in the first place for reasons of security and safety - to ensure the safety of themselves and their family members or to keep their home and property secure. In some cases though the vulnerabilities and problems reported by the users of these devices become, ironically, a new source of insecurity, anxiety and stress – stalkers digitally stalking the victim even at their intimate moments in their homes, and outsiders given unauthorised access to victim's property remotely.

Such hacking incidents becomes particularly problematic, dangerous and harmful when children are involved or affected by the incident. In one instance, a parent reported of a traumatic experience when they realised their child was potentially subjected to security camera hack. In this case, their child could hear voices from the camera installed in their bedroom assuming it was the parent asking them to act upon a presumably 'innocent' request:

"I just unplugged the camera in my child's room. This morning she came back in to wake me up and said the following: "Mom why did you talk on my speaker?" What? "You talked on my speaker." When? "Right now. You said hey go to sleep." Right now? "Yeah and I didn't like it. You said stop playing and go to sleep." I asked her if it was a mommy voice or a daddy voice, and she said mommy voice and then imitated it, whispering. And she said, "and I didn't like it so I covered my ears and came in here.["] I am FREAKED out and promptly went in her room and unplugged it".

While parents who reported this specific case, fortunately, did not report any other incident after they disconnected the device, several parents reported the terror of hearing a stranger's voice in their kid's room via a hacked baby monitor, threatening to kidnap and harm their child [83]. The use of such technology to hijack the authority of the system owner in the eyes of someone being cared for – be that a child or other dependants – can not only cause emotional and (potential) physical harm but echos many confidence scams and man in the middle hacks [29, 60] and opens the path for the same categories of maleficence.

5 Discussion: Rethinking Hacks

As work in the SOUPS community has explored [52, 75, 84], cybersecurity has political, social, psychological and economic aspects. We find this becomes more important if, as we do here, we attempt to focus not on the hacks themselves but on the people who the hacks have impact upon. By focusing on these hacked 'users', we have attempted here to open up a new front in understanding both how hacks operate and the ongoing impacts they have.

5.1 Designing for being hacked

The most common question that is brought to the online forums we studied was "have I been hacked?". At the heart of the user experience of hacking is users' own uncertainty in their need for help. This suggests that the needs of users for support go much beyond technically detecting and blocking a hack (useful though that would of course be), but of helping the user in this situation more broadly.

In terms of design, this points to a number of directions. Beyond basic security help and information [8], there is often a need for diagnosing particular issues with particular devices and listing unusual behaviours that might be mistaken for being signs of a hack. So for example, for each device or service tools could help by summarising others' experiences around suspecting or even being hacked. This could take the form of a knowledge base, or a tool that summarises forum interactions in some way. Such a knowledge base can offer a set of actions and tasks from which users could benefit from collecting evidence around the incident, their setup and any other data that often struggle to collect by themselves. Such data could help an outsider assist, be that law enforcement or security forensics, in diagnosing and assisting a hacking victim. This can be used as a design direction for supporting the manufacturer (or third party) providing support.

Indeed, it may be at times that what is needed is something that goes beyond direct support, yet also deals with their emotional needs. The forums themselves in different ways play a role here in that they provide a venue for support from others with dealing with the hack. The role they play is a sort of 'technical counselling' - with support spanning from help with the technology, of course, but also how the hack interferes with social relationships, assistance from the law, emotional support and even financial assistance. One interesting, and challenging, area of design would be to focus our attention on cases where users think they have been hacked but probably have not been hacked – what we called 'non-hacked hacks'. As we described above, it is not users' technical incompetence here that is to blame but often poor design decisions, as well as the inscrutability of IoT systems (that can only communicate with users through a flashing light without indicating a clear direction or purpose) can fail the user in detecting the problem or result in hypervigilant reactions towards unexpected actions. As technology is becoming more and more embedded in people's everyday lives, as our data suggested, there is a need for additional technical solutions that helps users with the fluidity and integration of maintenance of IoT devices in their homes. Receiving a push notification on users' mobile device can be one solution to help them understand if the flashing light is in fact related to an ongoing update or an indication of a hack.

Another suggestion to facilitate this approach is designing security tools that are tailored toward the needs of casual IoT users rather than network and security experts (e.g. [35]). A 'white hat' tool could communicate with other IoT devices located on the same network, scan logs and configurations to work out if there has likely been a hack, but also to broadly assist and reassure users who might be reasonably concerned by the unusual behaviour of their systems. While such a design can technically be complex (as it requires access to a set of diverse protocols and standards such as in [2]), designing for 'non-hacked hacks' might focus as much on reassuring users as detecting a hack. This could be as simple as documenting the different devices on a networks, and describing their usual failures and other unusual behaviours that other users have detected. While 'secure by design' has been a powerful guide in the cybersecurity world, it unfortunately removes users as active agents in the security process. In designing IoT security systems there may be opportunities for supporting users to go beyond what can be 'designed in' to a system as part of the development process. If we contrast technology with the case of automobiles, we can see how safety is not something that can be 'designed' during manufacture, it is an ongoing commitment supported by product recalls, testing institutes, safety certifications and so on. In this way we would argue for users' involvement in 'lifecycle security', where security comes from supporting users in detecting, repelling and dealing with being hacked throughout the life of a product.

5.2 Cybernoia

Our data lets us move beyond thinking about hacks as mainly technical objects – as something that can be prevented through better security – to thinking about them as users' experiences through how they discover and manage them, and in their relationships with others. Hacks exist not only as breaches in the security, but also breaches in the practices and understanding of end-users. Hacks by their very nature will always exist outside the knowledge and understanding of those who they impact, beyond the understanding of victims, at least initially. Preventing and supporting users then in dealing with hacks is not only a question of design or technical specification, but also one of supporting users' understanding and engagement with their systems when things go wrong.

Hacks can have a considerable psychological impact on users. There are unfortunate ways in which hacks can also contribute to, or be part of, ongoing mental health conditions suffered by the user. Paranoia - a feature of different mental health conditions - can lead to imagined hacks, but also the expansion of small mishaps or mistakes in a system to major incidents of victimisation. *Cybernoia* is a feature that may be ever more pressing as paranoia and technology use go together. This cybernoia is less frequently identified by the OPs, but usually it comes from posters who accuse the OP of inventing unlikely scenarios and being part of ridiculous 'tinfoil hat' conspiracy theories.

Yet as we have outlined here, there is the need to realise that hacks exist when they are perceived by users – even if they are actually not hacks as technically defined. In many situations users cannot determine themselves if they are actually hacked or not, with the sometimes bizarre behaviour of systems giving users a reasonable (if sometimes unreasonable) belief that they have been hacked. For these situations the impact is as if the user actually had been hacked - as the famous phrase puts it "things imagined are real in their consequences" [59].

5.3 Security and relationships

There are a number of recent papers that argue that cybersecurity needs to take an explicitly feminist direction in understanding how technology can become part of abuse and even enabling violence and discrimination [50, 58, 74]. Building on this, our data contributes to an understanding of how security is a practice embedded in users' relationships with others – the question of 'who' has hacked is as important as 'how' users were hacked. Indeed, the ways in which security is embedded in different social relationships that take place around IoT can create new forms of harm, insecurities and dependency.

Dealing with a hack necessarily involves going beyond ' expectations and current knowledge, requiring somewhat a level of trust. Thinking about the social aspects of hacks thus focuses attention on the relationships between the hacked and the hacker, between the organisations that make technical systems, and users who resort to different support resources to manage them. As our data shows, the forums we studied (and the users who contribute to them) play an important role in supporting users who find that the manufacturers have let them down in whatever way. Indeed, the level of support offered for much of the IoT that we focused on here can be rather poor and users found little support from either the organisations involved when their issues because serious. This led them to resort to Internet forums which can be seen as important sites to whoever tries to understand problems and to get support.

A different relationship which cybersecurity can become part of is that between family members. As a technology that is often used at home, IoT devices are frequently shared amongst family members. An Alexa smart speaker, for example, is available to everyone in the household and will be activated when the wake word is used regardless of users' age. Being 'shared by default' – sometimes just because they are physically in a shared family space – makes IoT potentially more useful, as something that goes beyond individual usage. But this also presents new challenges for IoT security since this becomes another aspect of devices that needs to be managed and shared across a family, with likely different users having a diverse set of security skills and knowledge of understanding how IoT ecosystems work and how the security is achieved. Maintaining 'home security' – in terms of IoT can then become a new point of dependency between household members, and at times then a new vulnerability for those who are newly dependent. Even if the technology itself tries to be diverse and accessible – affecting users without technical background [81] – it actually results in new unwanted dependencies and inequalities. While asynchronous knowledge and control over an IoT device can create whimsical and fun moments of playing pranks on other household residents, it also can result in exposing these residents "particularly women, to unique privacy and security risks." [76].

6 Conclusion

In this paper we have sought to return hack victims themselves to understand what it is to be hacked. Using online reports of hacks, we reviewed 210 self reports of hacks to identify the role that uncertainty plays, but also more broadly how users understand and deal with the experience of having their home IoT systems hacked in some way. Our focus on IoT lets us explore technologies which while still in flux, are increasingly embedded into our world and homes. Vulnerabilities in IoT are then especially worrying.

Indeed, the growth in their acceptance and use of IoT suggests that their use may not only because their use may become increasingly involuntary, but IoT may become as commonplace as ordinary 'non-smart' devices are today. This then means that the victims' stories that we identified here may move from unusual examples, to be a much more widespread phenomena. As we talk of 'early adopters' of technology, our users may actually be 'early victims', with their stories and experiences offering a broader warning about IoT and cybersecurity more generally.

In doing so we follow the long tradition in SOUPS of putting the social back into the technical - the hack as both as social and a technical object.

Acknowledgements

This research is partially funded by a Digital Futures postdoctoral research grant, and the Swedish Research Council (Vetenskapsrådet) under the project Securing Things (2017-04804: Säkra saker: Säkra sakernas Internet).

References

[1] Omnia Abu Waraga, Meriem Bettayeb, Qassim Nasir, and Manar Abu Talib. Design and implementation of automated IoT security testbed. *Computers & Security*, 88:101648, January 2020.

[2] Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac. Peek-a-boo: i see your smart home activities, even encrypted! In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '20, pages 207–218, New York, NY, USA, July 2020. Association for Computing Machinery.

[3] Katherine Albrecht and Liz Mcintyre. Privacy Nightmare: When Baby Monitors Go Bad [Opinion]. *IEEE Technology and Society Magazine*, 34(3):14–19, September 2015.

[4] Nazanin Andalibi, Oliver L. Haimson, Munmun De Choudhury, and Andrea Forte. Understanding Social Media Disclosures of Sexual Abuse Through the Lenses of Support Seeking and Anonymity. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 3906–3918, New York, NY, USA, May 2016. Association for Computing Machinery.

[5] Carmelo Ardito, Regina Bernhaupt, Philippe Palanque, and Stefan Sauer. Handling Security, Usability, User Experience and Reliability in User-Centered Development Processes. In David Lamas, Fernando Loizides, Lennart Nacke, Helen Petrie, Marco Winckler, and Panayiotis Zaphiris, editors, *Human-Computer Interaction – INTERACT 2019*, Lecture Notes in Computer Science, pages 759–762, Cham, 2019. Springer International Publishing.

[6] Paul Atkinson and David Silverman. Kundera's Immortality: The Interview Society and the Invention of the Self. *Qualitative Inquiry*, 3(3):304–325, September 1997.

[7] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3):210:1–210:27, January 2021.

[8] Brennen Bouwmeester, Elsa Rodríguez, Carlos Gañán, Michel van Eeten, and Simon Parkin. "The thing Doesn't Have a Name": Learning from emergent real-world interventions in smart home security. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 493–512. USENIX Association, August 2021.

[9] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, January 2006.

[10] Barry Brown, Stuart Reeves, and Scott Sherwood. Into the wild: Challenges and opportunities for field trial methods. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1657–1666. Association for Computing Machinery, New York, NY, USA, May 2011.

[11] Barry Brown, Minna Vigren, Asreen Rostami, and Mareike Glöss. Why users hack: Conflicting interests and the political economy of software. *Proceedings of the ACM on Human-Computer Interaction*, (CSCW), 2022.

[12] Barry Brown, Alexandra Weilenmann, Donald McMillan, and Airi Lampinen. Five Provocations for Ethical HCI Research. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 852–863. Association for Computing Machinery, New York, NY, USA, May 2016.

[13] Amy Bruckman, Kurt Luther, and Casey Fiesler. When Should We Use Real Names in Published Accounts of Internet Research? In *Digital Research Confidential: The Secrets of Studying Behavior Online*, pages 243–258. MIT Press, 2016.

[14] Mark Button, Dean Blackbourn, Lisa Sugiura, David Shepherd, Richard Kapend, and Victoria Wang. From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, 64:101675, November 2021.

[15] Mark Button and Cassandra Cross. *Cyber Frauds, Scams and Their Victims*. Routledge, London, May 2017.

[16] Rainara M. Carvalho, Rossana M.C. Andrade, Káthia M. Oliveira, and Christophe Kolski. Catalog of Invisibility Requirements for UbiComp and IoT Applications. In *2018 IEEE 26th International Requirements Engineering Conference (RE)*, pages 88–99. IEEE, August 2018.

[17] Anna C. Cavender, Daniel S. Otero, Jeffrey P. Bigham, and Richard E. Ladner. Asl-stem forum: Enabling sign language to grow through online collaboration. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2075–2078. Association for Computing Machinery, New York, NY, USA, April 2010.

[18] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp '12, pages 61–70, New York, NY, USA, September 2012. Association for Computing Machinery.

[19] E. Gabriella Coleman. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton University Press, Princeton, December 2012.

[20] Dan Conway, Ronnie Taib, Mitch Harris, Kun Yu, Shlomo Berkovsky, and Fang Chen. A Qualitative Investigation of Bank Employee Experiences of Information Security and Phishing. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 115–129, 2017.

[21] Cassandra Cross. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2):187–204, May 2015.

[22] Cassandra Cross, Megan Parker, and Daniel Sansom. Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. *International Review of Victimology*, 25(1):53–69, January 2019.

[23] Brittany D. Davis, Janelle C. Mason, and Mohd Anwar. Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal*, 7(10):10102–10110, October 2020.

[24] Paul Dourish, Rebecca E. Grinter, Jessica Delgado De La Flor, and Melissa Joseph. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 2004.

[25] Brianna Dym and Casey Fiesler. Ethical and privacy considerations for research using online fandom data. *Transformative Works and Cultures*, 33, June 2020.

[26] Milène Fauquex, Sidhant Goyal, Florian Evequoz, and Yann Bocchi. Creating people-aware IoT applications by combining design thinking and user-centered design methods. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 57–62, December 2015.

[27] Jessica L. Feuston and Anne Marie Piper. Everyday Experiences: Small Stories and Mental Illness on Instagram. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–14, New York, NY, USA, May 2019. Association for Computing Machinery.

[28] Casey Fiesler and Nicholas Proferes. "participant" perceptions of twitter research ethics. *Social Media + Society*, 4(1):2056305118763366, 2018.

[29] Peter Fischer, Stephen E. G. Lea, and Kath M. Evans. Why do individuals respond to fraudulent scam communications and lose money? the psychological determinants of scam compliance. *Journal of Applied Social Psychology*, 43(10):2060–2072, 2013.

[30] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. A Stalker's Paradis: How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 1–13, New York, NY, USA, April 2018. Association for Computing Machinery.

[31] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):46:1–46:22, December 2017.

[32] Márcio Miguel Gomes, Rodrigo da Rosa Righi, and Cristiano André da Costa. Future directions for providing better IoT infrastructure. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, UbiComp '14 Adjunct, pages 51–54, New York, NY, USA, September 2014. Association for Computing Machinery.

[33] Colin M. Gray, Shruthi Sai Chivukula, and Ahreum Lee. What Kind of Work Do "Asshole Designers" Create? describing Properties of Ethical Concern on Reddit. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, pages 61–73, Eindhoven Netherlands, July 2020. ACM.

[34] Xinning Gui, Yubo Kou, Kathleen H. Pine, and Yunan Chen. Managing Uncertainty: Using Social Media for Risk Assessment during a Public Health Crisis. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 4520–4533, New York, NY, USA, May 2017. Association for Computing Machinery.

[35] Hassan Habibi Gharakheili, Arunan Sivanathan, Ayyoob Hamza, and Vijay Sivaraman. Network-Level Security for the Internet of Things: Opportunities and Challenges. *Computer*, 52(8):58–62, August 2019.

[36] Richard Harper, editor. *Inside the Smart Home*. Springer-Verlag, London, 2003.

[37] Billy Henson, Bradford W. Reyns, and Bonnie S. Fisher. Cybercrime victimization. In *The Wiley Handbook on the Psychology of Violence*, pages 555–570. Wiley Blackwell, Hoboken, NJ, US, 2016.

[38] Thomas Holt, Deborah Strumsky, Olga Smirnova, and Max Kilger. Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*, 6, January 2012.

[39] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13. Association for Computing Machinery, New York, NY, USA, April 2020.

[40] Jina Huh. Clinical Questions in Online Health Communities: The Case of "See your doctor" Threads. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '15, pages 1488–1499, New York, NY, USA, February 2015. Association for Computing Machinery.

[41] Jina Huh and Wanda Pratt. Weaving clinical expertise in online health communities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 1355–1364, New York, NY, USA, April 2014. Association for Computing Machinery.

[42] Max Ingham, Jims Marchang, and Deepayan Bhowmik. IoT Security Vulnerabilities and Predictive Signal Jamming Attack Analysis in LoRaWAN. *IET Information Security*, January 2020.

[43] Andreas Jacobsson and Paul Davidsson. Towards a model of privacy and security for smart homes. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 727–732, December 2015.

[44] Tim Jordan and Paul Taylor. A Sociology of Hackers. *The Sociological Review*, 46(4):757–780, November 1998.

[45] P. Karthika, R. Ganesh Babu, and P. A. Karthik. Fog Computing using Interoperability and IoT Security Issues in Health Care. In Devendra Kumar Sharma, Valentina Emilia Balas, Le Hoang Son, Rohit Sharma, and Korhan Cengiz, editors, *Micro-Electronics and Telecommunication Engineering*, Lecture Notes in Networks and Systems, pages 97–105, Singapore, 2020. Springer.

[46] Megan Knittel, Faye Kollig, Abrielle Mason, and Rick Wash. Anyone else have this experience: Sharing the Emotional Labor of Tracking Data About Me. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):79:1–79:30, April 2021.

[47] Cliff Lampe, Rick Wash, Alcides Velasquez, and Elif Ozkaya. Motivations to participate in online communities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1927–1936. Association for Computing Machinery, New York, NY, USA, April 2010.

[48] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. Alexa, Are You Listening? privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):102:1–102:31, November 2018.

[49] Derek Layder. *Sociological Practice: Linking Theory and Social Research*. SAGE, September 1998.

[50] Roxanne Leitão. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, DIS '19, pages 527–539, New York, NY, USA, June 2019. Association for Computing Machinery.

[51] Eric Rutger Leukfeldt, R. J. (Raoul) Notté, and M. (Marijke) Malsch. Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims & Offenders*, 15(1):60–77, January 2020.

[52] Karen Levy and Bruce Schneier. Privacy Threats in Intimate Relationships. SSRN Scholarly Paper ID 3620883, Social Science Research Network, Rochester, NY, June 2020.

[53] Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. 'Internet of Things': How Abuse is Getting Smarter. SSRN Scholarly Paper ID 3350615, Social Science Research Network, Rochester, NY, March 2019.

[54] Diana MacLean, Sonal Gupta, Anna Lembke, Christopher Manning, and Jeffrey Heer. Forum77: An Analysis of an Online Health Forum Dedicated to Addiction Recovery. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '15, pages 1511–1526, New York, NY, USA, February 2015. Association for Computing Machinery.

[55] Lena Mamykina, Drashko Nakikj, and Noemie Elhadad. Collective Sensemaking in Online Health Forums. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 3217–3226. Association for Computing Machinery, New York, NY, USA, April 2015.

[56] Michael Massimi, Jackie L. Bender, Holly O. Witteman, and Osman H. Ahmed. Life transitions and online

health communities: Reflecting on adoption, use, and disengagement. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '14, pages 1491–1501, New York, NY, USA, February 2014. Association for Computing Machinery.

[57] Nora McDonald, Karla Badillo-Urquiola, Morgan G. Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J. Wisniewski. Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI EA '20, pages 1–8, New York, NY, USA, April 2020. Association for Computing Machinery.

[58] Dana McKay and Charlynn Miller. Standing in the Way of Control: A Call to Action to Prevent Abuse through Better Design of Smart Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, pages 1–14, New York, NY, USA, May 2021. Association for Computing Machinery.

[59] Robert K. Merton. The Thomas Theorem and the Matthew Effect. *Social Forces*, 74(2):379–422, 1995.

[60] Gopi Nath Nayak and Shefalika Ghosh Samaddar. Different flavours of Man-In-The-Middle attack, consequences and feasible solutions. In *2010 3rd International Conference on Computer Science and Information Technology*, volume 5, pages 491–495, July 2010.

[61] Andrea Grimes Parker, Ian McClendon, Catherine Grevet, Victoria Ayo, WonTaek Chung, Veda Johnson, and Elizabeth D. Mynatt. I am what i eat: Identity & critical thinking in an online health forum for kid. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2437–2446. Association for Computing Machinery, New York, NY, USA, April 2013.

[62] Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. In *Proceedings of the New Security Paradigms Workshop*, NSPW '19, pages 1–15, New York, NY, USA, September 2019. Association for Computing Machinery.

[63] Kari Paul. Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs. *The Guardian*, December 2020.

[64] James Pierce. Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–14. Association for Computing Machinery, New York, NY, USA, May 2019.

[65] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. Somebody's Watching Me? assessing the Effectiveness of Webcam Indicator Lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1649–1658. Association for Computing Machinery, New York, NY, USA, April 2015.

[66] Nicholas Proferes, Naiyan Jones, Sarah Gilbert, Casey Fiesler, and Michael Zimmer. Studying Reddit: A Systematic Overview of Disciplines, Approaches, Methods, and Ethics. *Social Media + Society*, 7(2):20563051211019004, April 2021.

[67] Sabirat Rubya and Svetlana Yarosh. Video-Mediated Peer Support in an Online Community for Recovery from Substance Use Disorders. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, pages 1454–1469, New York, NY, USA, February 2017. Association for Computing Machinery.

[68] Harvey Sacks. On doing "being ordinary". In J. Maxwell Atkinson, editor, *Structures of Social Action*, Studies in Emotion and Social Interaction, pages 413–429. Cambridge University Press, Cambridge, 1985.

[69] Harvey Sacks. Spring 1968: April 24 Second Stories. In *Lectures on Conversation Volume I (Edited by Gail Jefferson)*, chapter 7, pages 749–805. John Wiley & Sons, Ltd, 1995.

[70] Mattia Samory, Vincenzo-Maria Cappelleri, and Enoch Peserico. Quotes Reveal Community Structure and Interaction Dynamics. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, pages 322–335, New York, NY, USA, February 2017. Association for Computing Machinery.

[71] Amirali Sanatinia and Guevara Noubir. OnionBots: Subverting Privacy Infrastructure for Cyber Attacks. In *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 69–80, June 2015.

[72] Pedro Sanches, Vasiliki Tsaknaki, Asreen Rostami, and Barry Brown. Under Surveillance: Technology Practices of those Monitored by the State. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13. Association for Computing Machinery, New York, NY, USA, April 2020.

[73] Mike Simmonds. How businesses can navigate the growing tide of ransomware attacks. *Computer Fraud & Security*, 2017(3):9–12, March 2017.

[74] Julia Slupska. Safe at Home: Towards a Feminist Critique of Cybersecurity. SSRN Scholarly Paper ID 3429851, Social Science Research Network, Rochester, NY, May 2019.

[75] Julia Slupska, Scarlet Dawson Dawson Duckworth, Linda Ma, and Gina Neff. Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI EA '21, pages 1–6, New York, NY, USA, May 2021. Association for Computing Machinery.

[76] Yolande Strengers and Jenny Kennedy. *The Smart Wife: Why Siri, Alexa, and Other Smart Home Devices Need a Feminist Reboot*. MIT Press, Cambridge, MA, USA, September 2020.

[77] Lisa Sugiura, Rosemary Wiles, and Catherine Pope. Ethical challenges in online research: Public/private perceptions. *Research Ethics*, 13(3-4):184–199, July 2017.

[78] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[79] Huixin Tian, Chris Kanich, Jason Polakis, and Sameer Patil. Tech Pains: Characterizations of Lived Cybersecurity Experiences. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pages 250–259, September 2020.

[80] Orly Turgeman-Goldschmidt. Hackers' Accounts: Hacking as a Social Entertainment. *Social Science Computer Review*, 23(1):8–23, February 2005.

[81] EQUALS Skills Coalition UNESCO. I'd blush if I could: Closing gender divides in digital skills through education, 2019.

[82] Johan van Wilsem. Hacking and Harassment—Do They Have Something in Common? comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice*, 29(4):437–453, November 2013.

[83] Amy B Wang. Nest cam security breach: A hacker took over a baby monitor and broadcast threats, Houston parents say - The Washington Post. 2018.

[84] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 1–16, New York, NY, USA, July 2010. Association for Computing Machinery.

[85] Rick Wash. How Experts Detect Phishing Scam Emails. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):160:1–160:28, October 2020.

[86] Rick Wash and Molly M. Cooper. Who Provides Phishing Training? facts, Stories, and People Like Me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–12. Association for Computing Machinery, New York, NY, USA, April 2018.

[87] Meredydd Williams, Jason R. C. Nurse, and Sadie Creese. Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, pages 181–18109, August 2017.

[88] Peter Worthy, Ben Matthews, and Stephen Viller. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, DIS '16, pages 427–434, New York, NY, USA, June 2016. Association for Computing Machinery.

[89] Ibrar Yaqoob, Ejaz Ahmed, Muhammad Habib ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-garadi, Muhammad Imran, and Mohsen Guizani. The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, 129:444–458, December 2017.

[90] Randall Young, Lixuan Zhang, and Victor R. Prybutok. Hacking into the Minds of Hackers. *Information Systems Management*, 24(4):281–287, October 2007.

[91] Eric Zeng, Shrirang Mare, and Franziska Roesner. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, SOUPS '17, pages 65–80, USA, July 2017. USENIX Association.

[92] Leah Zhang-Kennedy, Hala Assal, Jessica Rocheleau, Reham Mohamed, Khadija Baig, and Sonia Chiasson. The aftermath of a crypto-ransomware attack at a large academic institution. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 1061–1078, 2018.

[93] Jane Y. Zhao, Evan G. Kessler, Jihnhee Yu, Kabir Jalal, Clairice A. Cooper, Jeffrey J. Brewer, Steven D. Schwaitzberg, and Weidun Alan Guo. Impact of Trauma Hospital Ransomware Attack on Surgical Residency Training. *Journal of Surgical Research*, 232:389–397, December 2018.

[94] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):200:1–200:20, November 2018.

Appendix A

Table 1: List of forums and subreddited

/r/homedefense	/r/talesfromtechsupport
/r/wyzecam	/r/cybersecurity
/r/Ring	/r/PS4
/r/HomeNetworking	/r/HayDay
/r/hacking	/r/privacy
/r/blinkcameras	/r/LegalAdviceUK
/r/raisedbynarcissists	/r/sonos
/r/nosleep	/r/homesecurity
/r/Hue	/r/ChoosingBeggars
/r/homeautomation	https://www.amazonforum.com
/r/galaxys10	https://community.norton.com/en/forums
/r/techsupport	https://forums.tomsguide.com
/r/smarthome	https://security.stackexchange.com/questions
/r/talesfromcallcenters	https://community.bt.com
/r/hometheater	https://forum.telus.com
/r/samsung	https://discussions.apple.com
/r/bravia	https://www.bleepingcomputer.com/forums
/r/dataisbeautiful	https://forum.level1techs.com/
/r/teslamotors	https://en.community.sonos.com
/r/Chromecast	https://answers.microsoft.com/en-us/xbox/forum
/r/googlehome	https://forums.wyzecam.com
/r/NoStupidQuestions	https://community.ring.com/
/r/funny	https://www.amazon.com/gp/customer-reviews/
/r/mildlyinteresting	https://forum.yitechnology.com/
/r/appletv	https://forums.wyzecam.com/
/r/PlayStationPlus	https://forums.tesla.com/discussion
/r/PewdiepieSubmissions	https://support.google.com/chromecast
/r/amazonecho	https://us.community.samsung.com
/r/alexa	https://community.blinkforhome.com
/r/googlehome	https://community.tp-link.com
/r/cybersecurity	https://lgcommunity.us.com/discussion
/r/techsupport	https://teslamotorsclub.com/

Appendix B

Table 2: Main categories of hacked devices with examples

Category	**Example**
Smart home devices	Amazon echo, Echo dot, Chromecast, Google home, Hue lights
Router and wifi	Archer C1200
Accounts, Game console and computers	Google account, Xbox, PS4
Smart locks	Ring doorbell
Phones and tablets	Apple, Samsung
Printer	Variety of models
Security camera	Wayz, Yi, Ring, Arlo
Smart speaker	Sonos
Smart tv	Sony, LG
Vehicle	Tesla

Table 3: Examples of high level codes. Note that each code can have multiple sub-codes and each post can be assigned multiple codes

Action taken	Hacker_family
Addressing the hacker	Hacker_neighbour
Addressing the manufacturer	Hacker_suspecious
Analysis of the hack	Hacker_unknown
Asking help from the forum	Harm
Comments on forum culture	Innovative tactics to solve the problem
Creepiness	Jokes
Paranoia	Lack of tech expertise with IoT
Cybersecurity	Manufacturer reply
Cybersecurity education	Hacker_expartner
Debating cybersecurity	Mental health
Description of the problem	Not a hack but
Distrust in police help	Other evidence
Evidence of the hack	Own expertise
Existing security practice	Paranoia
Forum reply_advice	Reasons to have the device
Forum reply_analysis of the hack	Shaming_questioning
Forum reply_comments on cybersecurity	Sharing own cybersecurity practices
Forum reply_debating other reply	Sharing own story
Forum reply_doubting the story	Type of post_asking for help
Forum reply_sharing own hacking story	Type of post_attention from manufacturer
Getting back at the hacker	Type of the device
Hacker_partner	What happened_the hack