Social Media as a Resource for Understanding Security Experiences: A Qualitative Analysis of #Password Tweets

Paul Dunphy[1], Vasilis Vlachokyriakos[1], Anja Thieme[1], James Nicholson[1],
John McCarthy[2], Patrick Olivier[1]
[1] Culture Lab, School of Computing Science, Newcastle University
[2] School of Applied Psychology, University College Cork
1{forename.surname}@ncl.ac.uk, 2john.mccarthy@ucc.ie

ABSTRACT

As security technologies become more embedded into people's everyday lives, it becomes more challenging for researchers to understand the contexts in which those technologies are situated. The need to develop research methods that provide a lens on personal experiences has driven much recent work in human-computer interaction, but has so far received little focus in usable security. In this paper we explore the potential of the micro blogging site *Twitter* to provide experience-centered insights into security practices. Taking the topic of passwords as an example, we collected tweets with the goal to capture personal narratives of password use situated in its context. We performed a qualitative content analysis on the tweets and uncovered: how tweets contained critique and frustration about existing password practices and workarounds; how people socially shared and revoked their passwords as a deliberate act in exploring and defining their relationships with others; practices of playfully bypassing passwords mechanisms and how passwords are appropriated in portrayals of self. These findings begin to evidence the extent to which passwords increasingly serve social functions that are more complex than have been documented in previous research.

1. INTRODUCTION

Nearly twenty years have passed since early calls for usable security [40] where security researchers were encouraged to lend contemporary research methods from the field of human-computer interaction (HCI). The HCI methods of the day were focused upon improving the efficiency of users in their interactions with digital technology in the workplace; however, even at that point in time, digital technologies were already accelerating on a trajectory of becoming tightly interwoven into people's everyday lives. Designing and evaluating digital technologies that will play this role is challenging, because the success criteria for that technology is not only related to the efficiency of the interface interactions but must include a broader agenda of understanding how technologies involve people emotionally, intellectually and sensually [24].

It is challenging to understand and design for these facets of technology usage as people appropriate technologies differently according to their own personal circumstances, past experiences and anticipations for the future. However, engaging with this challenge and taking an experience-centered [39] approach to design requires designers to continuously seek new perspectives on how people live with the technologies they design [27] and accept that interactions and experiences are unique to the person through their own interpretations, feelings and value judgments [25]. By trying to see the world through the eyes of another person and respecting the different values held by others, the designer is better placed to generate a rich, contextual understanding of the problem at hand as well as new design ideas. Recent work has argued the value of a focus of an experience-centered approach to usable privacy and security [9], but while some research is beginning to address this challange [29, 36] there is still a dearth of methods for eliciting, evoking and developing descriptions of everyday security experiences.

Social media platforms are used by people to share their thoughts and opinions with friends, family, colleagues, or others with similar interests. Communicating online, people exchange information via 'posts'; an important attribute of these posts is that they are made in a naturalistic setting and in the course of daily activities. The content of these posts is increasingly the focus of analysis for those seeking to better understand people's behaviors and opinions, ranging from understanding political sentiment [2], to tracking the spread of the flu virus [22]. However, while platforms such as Twitter —used for everyday conversations, the sharing of news, and to document daily occurrences [17] —had a user base of 232 million at the end of 2013 [28], no work has yet investigated its potential as a resource of everyday security experiences, nor considered how data of such scope and scale might enhance our understanding of how people appropriate security mechanisms into their lives.

To these ends, this paper makes two key contributions to the study of security experiences: firstly we identify social media, specifically Twitter, as a resource of naturally generated reflections on security practices and workarounds in social settings, and qualitative content analysis (QCA) as an appropriate method of analysis. Secondly, analyzing tweets on the topic of the password we identify key qualitative themes and present data that provide new perspectives on everyday password usage situated within the context and complexity of everyday life, social relations, and practices.

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

2. RELATED WORK

2.1 Understanding Password Practices

Conventional wisdom on managing passwords securely has not changed much since early guidelines were published [3]. Such guidelines are typically centred upon changing passwords regularly, not sharing passwords with others, not writing them down, and making them difficult to guess for others. Much work has taken place in the usable security community to understand how desired password behaviors (set out in guidelines) manifest in practice. Klein [19] showed that people were likely to choose very short passwords that were vulnerable to guessing attacks structured by a standard word dictionary. Sasse et al. [30] conducted a survey in a workplace and uncovered the challenges people faced to remember passwords; particularly those that were infrequently used. This work also highlighted that the requirements of securely managing passwords had considerable potential to conflict with everyday work practices.

Password sharing is a topic that recurs in studies both in and out of the workplace. Inglesant and Sasse [15] report that shared passwords were a de facto means to access shared resources in the workplace. Outside of the workplace, the literature is more sparse. Kaye [18] reports the results of a survey that describe how passwords were routinely, yet thoughtfully, shared amongst partners and spouses, friends and family and even work colleagues. Indeed, one third of respondents claimed to share their personal email password, compared to one quarter sharing their Facebook password; in both cases sharing was predominantly with partners and close friends. Examples that could be considered more extreme shed light on the how people share passwords to overcome physical or geographical difficulties. Dunphy et al. [8] report how older adults would delegate personal identification numbers (PINs) to helpers who would visit the ATM on their behalf. Singh et al. [32] describe occurrences of password sharing amongst couples but also report how an entire village would delegate bank credentials to a single person who would travel a considerable distance to the nearest bank to conduct business on everybody's behalf.

Each of the presented research studies represent considerable investments in time to work together with user groups 'in the wild' to surface relevant insights. However, while it may be attractive to dismiss some of the examples as particularly extreme, the reality is that for the people living in those contexts, the practices are completely normal and represent a very personal and experience-centered trade-off between usability and security.

2.2 Understanding People via Social Media

Piskorski [28] explains that people are attracted to social media platforms as they offer different ways to interact with others and help fulfill social needs. Twitter is a micro blogging-based social network site that is arguably the most popular example of its kind; it grew in popularity around 2010. The platform offers functionality to connect to strangers, yet it provides some opportunities for interactivity or more private communication with friends. Morris et al. [26] describe how Twitter is used to distribute content such as breaking news, describing the platform not only as a social network, but also as a news source that people access to specifically search for a topic of personal or community interest. Duggan and Smith [7] published a survey report about social media use by Americans, which showed that about 18% of all online adults are Twitter users, compared to the 71% being users of Facebook the largest online social platform. While Facebook is popular across a range of demographic groups, 31% of Twitter users are drawn from the age range 18-29 (19% of Twitter users are in the age range 30-49 years; 9% for 50-64 years; 5% for 65+ years) with a particular presence of urban dwellers, African-Americans and Hispanics. Moreover, Twitter users are split equal in gender and 46% of all Twitter users tend to visit the site daily (29% multiple times per day). Smith and Brenner [33] further reported on a high correlation between the use of Twitter and of mobile technology, especially smartphones, which is generally high among African Americans and Hispanics, and is an increasing trend amongst younger adults.

The challenge to understand peoples' behaviors and opinions outside of the laboratory context in a resource respectful manner is faced by a multitude of researchers. One approach that is increasingly popular concerns the analysis of social media posts as empirical data. For example, Kramer [20] analyzed posts from Facebook and applied techniques of quantitative sentiment analysis to explore the measurement of levels of happiness in the user group. Lampos and Cristianini [22] used a content analysis of tweets to estimate the spread of the H1N1 virus in the UK; their estimates showed a fair agreement with the estimates of central government at the time. Golder and Macy [11] found that social media posts can mirror seasonal behavior fluctuations across different communities. Moreover, social media (specifically Twitter) has been used in the last few years to monitor political sentiment and predict election results [2, 33]. While communication and politics researchers have contrasting views on the validity of Twitter for these purposes —mainly due to concerns around the representativeness of the sample —Twitter has shown itself to be an reasonable predictor of election results (e.g. as an exit poll) when both volume-based measures and sentiment analysis are applied [35].

The analysis of posts on social media platforms has so far served a variety of purposes in the field of human-computer interaction. For example, the act of tweeting is increasingly integrated into large events or even television shows as a way to encourage audience participation, gather feedback, or provoke debate. Doughty et al. [5] analyzed tweets published during a UK-based television show that focused upon the Irish traveler community. They discuss how the tweet contents demonstrated the potential for Twitter to reveal prejudices held by an audience, but also how the micro blogging might have served to reinforce those prejudices.

3. SOCIAL MEDIA AND SECURITY EXPERIENCES

Social media analysis has not yet been considered as a means to understand everyday experiences of security technologies. When considering why we might need new methods to specifically capture naturalistic everyday experiences, it is important to note the two types of knowledge that researchers may aim to elicit from users through research: *explicit knowledge*, and *tacit knowledge* [39]. Explicit knowledge comprises that which is easy to transmit to another person e.g. the number of siblings a person may have, or the number of passwords that a person uses. Much of what we

know about the world however is tacit knowledge; knowledge that is difficult to transfer to another person e.g. how to use complex equipment (where experience has guided learning), or reasons for why a system feels secure.

Accessing tacit knowledge typically requires researchers to apply a mix of methods in their interactions with people (e.g. observations, surveys, diaries etc.) to identify and capture instances of interesting behaviors, and may even include working together with participants to highlight that interesting behaviors exist in the first place, but also to understand why those behaviors come about [38]. Relatively few methods in usable security go beyond traditional interviews and surveys to elicit this tacit knowledge; these classic methods best serve as tools to capture explicit knowledge (except where *dialog* [39] is explicitly supported), as do allow respondents to reflect on their own behaviors, however, within an experimenter defined framework.

The use of social media posts as a lens on everyday security experiences would immediately present a number of methodological benefits:

- People are free to use their own vocabulary to describe their feelings and practices.
- Posts are created in naturalistic contexts and in the course of everyday activities.
- Security would be positioned as a social and collective [6] practice rather than a personal and secretive practice.
- There is a large volume of social media posts to study, and they are typically short in length.

3.1 Everyday Vocabulary

Despite the common mantra that users are not interested in security, recent research suggests that, at times, users give it the utmost care and attention [18]. However, people might not describe their concerns or understanding in ways that experts would immediately recognize. As security features permeate the everyday technologies that people encounter, security becomes more of a subject of public discourse and people are able to collectively develop their own ways to articulate concerns as security becomes a less guarded topic. This vocabulary can spread across communities in the form of colloquial language or even form folk stories [36]. Indeed, this expert-oriented lexicon around security is likely to be one of the reasons why it can be challenging to support people to contribute effectively to conversations around information security.

3.2 Naturalistic Insights

Social media posts can be created in the course of everyday living where participants are taking part in neither a lab nor a field study, which frees the data from biases introduced by a researcher or by a specific topic under investigation. For typical people there can be many reasons to create personal social media profiles to document their everyday lives, however, one of those reasons is unlikely to be to purely discuss security or privacy (although this is possible). Consequently, we can think of social media as a side channel into everyday life where personal experiences are foregrounded. This approach can mitigate biases introduced by the researcher that occur naturally in a face-to-face scenario such as pursuing personal interests or directing conversations towards active hypotheses. Of course, alleviating the biases introduced by a researcher in a face-to-face context does not imply that the data are not skewed in any other way (see Limitations and Related Work) or that eliminating all bias is desirable. Indeed, by focusing upon experiences we are placing personal biases of users as the core item of enquiry; micro-blogging sites have been designed to allow fast and concise user interaction and are designed to support users' self-portrayal. As a result, the affordances of the social media platform have an effect on people's interactions and the types of posts they may make.

3.3 Security as a Collective Practice

Information security behaviors are typically considered at the level of the individual. Social media platforms encourage social interactions; so far researchers have studied social media posts and have succeeded mainly in generating insights relating to group behavior [2, 33]. While research documenting group security behaviors does exist e.g. [32, 8, 18], this strand of work is still underexplored and chiefly serves to provide contrast to the mainstream research agenda focused upon the individual; evidenced by the observation that insights from such studies are slow to find their way into proposed system designs. The existence of security-related experiences on social media could help redress the balance and provide opportunities to study diverse online communities and better understand how security is appropriated in such groups. A group perspective on a security technologies could provide opportunities to question how a technology 'should' be used, and shed new light on the ways in which security is actually socially practiced and negotiated.[6].

3.4 Big Data of Security Experiences

It is reported that 500 million tweets are posted per day on Twitter [1]. The sheer volume of social media posts online lends itself to a number of methods of data analysis both qualitative and quantitative. In this paper we take a qualitative approach which reflects our contention that personal experiences can be complicated and personal, however, other methods exist which can support the data analysis process or the filtering down of a large dataset such as *sentiment analysis* [34]; this is one quantitative method widely used in social computing and provides one perspective on the overall mood in the data according to the identification of positive and negative word combinations. While the social media data is owned by a private company, the data is openly searchable which can provide a certain element of transparency in the sourcing of data and comparisons across online communities, even at different points in time according to events that happen in society. Research across a number of disciplines is pursuing methods to aid exploration of large quantities of data, but open questions would remain around feeding insights back into the design of security technologies.

4. STUDY METHOD

Over a period of 26 days in February 2014 we collected password-related tweets using the Twitter Search API (this preceded the streaming API which is now widely used). Our search criteria returned all available tweets containing the hashtag '#password' or the keyword 'password', in combination with searches that additionally included specific pronouns e.g. 'I', 'me', 'you', and possessive pronouns e.g. 'my', 'your'. This was to ensure that tweets were as closely re-

lated as possible to personal experiences. The search criteria would also return replies to tweets containing that criteria and retweets. During the time period of the study, we downloaded the most recent 15 'pages' of tweets each hour, using individual timestamps as a check to determine whether we had downloaded a particular tweet before. Our focus was on tweets with unique content, so after one pass to filter out retweets, our dataset comprised just over 500,000 tweets ($\mu = 19222$ per day, $\sigma = 3623$). This relatively large dataset indicates a common occurrence of password-related discussion within daily communications on Twitter.

4.1 Data Analysis

The approach of our research was qualitative. We conducted a Qualitative Content Analysis (QCA) [21] on a sample of 1000 tweets that were randomly selected from the dataset, and were roughly balanced across each day of data collection. We chose QCA over alternative approaches such as Grounded Theory [10], since our research is exploratory in nature, with a focus on latent expressions of personal experiences (inductive) and led by existing theories and previous research on peoples' password practices (deductive).

For our QCA, three members of the research team independently familiarized themselves with the data to identify and systematically search for (reccurring) themes in the tweets. Identified themes were then coded, first individually and then recoded following conversations between the researchers, and then synthesized to higher-level categories. The comparing of content codes and discussing them with each other formed an essential part in this process, since, for a large number of the tweets, and influenced by our individual perspectives, multiple interpretations and thematic groupings seemed possible. Partly, this was due to a lack of context information that was available in relation to each tweet, which in itself provided little insights about the situation that may have motivated the post, or the intentions of the person sending the message. For some messages it was also not always clear if they were intended to reflect a serious statement or an expression of sarcasm or a joke, leading us to be particularly cautious in their interpretation. After one pass of our QCA we disregarded 302 tweets from further inquiry, as they were either not written in English (124 tweets); presented advertisement or spam messages (52 tweets); were unreadable (e.g. cryptic composition of numbers or characters; 29 tweets); or presented posts that were ambiguous (97 tweets) to the extent that the researchers could not reach agreement about their content. The remaining 698 tweets that were conclusive and agreed on by all three coders were analyzed with regard to the insights they provide for understanding peoples' password practices and concerns. Although we could have included more tweets, we noticed towards the end of our analysis that the themes that we had identified reached saturation, whereby any additional tweets only provided more examples of a similar themes. Our findings present the themes that evolved through this mode of analysis.

4.2 Limitations

Before the presentation of our findings, it is worth clarifying some limitations of the data that will be presented. From an analysis perspective, we disregarded tweets that were not written in English. At the time of our study, The Twitter Search API allowed the retrieval of at most a 1% of all the data matching some specified criteria. After the threshold of 1% has been reached only sampled data is available to the API calls of the user, with the methods of sampling unknown (although premium search options did exist). Such restrictions may be removed in the newer Streaming API. As with any online community there are discrepancies in which members make the biggest contributions; on Twitter, some estimates suggest that 40% of users do not tweet at all, and 90% have less than 10 tweets [14]. Secondly, as with any qualitative data, the data we present should not be scrutinized for its generalizability. The data provides insights confined to the group of people it was collected from and the reader should consider the transferability of the insights with caution. As such, the reader should scrutinize the data for its trustworthiness [12], which is composed of credibility, transferability, dependability, and confirmability.

5. FINDINGS

Our QCA revealed three high level themes. Firstly, people commonly tweeted about specific practical difficulties that they encountered in the set-up or retrieval of passwords; how they experienced such difficulties, as well as a range of individual workarounds they developed to manage these; all of which highlight classic usability and security issues. Secondly, tweets contained insights into some of the complexities that surround peoples' everyday uses of passwords within their social life. In this regard, users expressed how the request, receipt and sharing of passwords with others assisted in exploring and defining a person's relationship with others. Thirdly, some tweets served to portray the personality of a person in a certain light, where the password was used to reinforce certain desired aspects of a person's character. Thus, the final theme presents how people made use of their understanding of, and practices around, their use of passwords to support a specific display of identity.

The particular passwords that people appeared to discuss were mostly online accounts such as social media sites, video-streaming services, and so forth. This might indicate that Twitter is an adequate platform for understanding the experiences of these types of (more social) passwords, or it might be our search criteria were inadequate for collecting insights on other types of password. In the following sections we provide example tweets that illustrate our three themes. How these initial observations can be interpreted is then developed further in the discussion section of the paper.

5.1 Password Practices and Workarounds

One third of the tweets that we analyzed ($n = 237$, 34%) presented descriptive accounts of the difficulties that people encountered in generating, remembering and recovering their passwords. Even though this could have been expected considering the search criteria that we used to collect the tweets, it is particularly interesting that these accounts were also followed by feelings of anxiety and frustration about a potential loss of access to one's account, as well as some of their personal strategies for managing these.

5.1.1 Frustration about System Demands for Secure Practices

In a number of tweets ($n = 87$, 12%) users expressed, often in a sarcastic or joking manner, their opinion about current requirements posed upon them in the creation of secure passwords for their accounts. They expressed critique

about demands to generate passwords that are very long, include upper or lower case characters, and a number, and to also have to change and to re-enter these frequently. Users tweeted for example: *"Sorry your password must contain a capital letter, two numbers, a symbol, and a inspiring message #BumpDat"*; *"I thought it'll be a password not a passspeech"*; *"It's always a test of my intelligence when I change my password"*; or *"Why must I type in my Apple ID password EVERY TIME I download an app?!? #Annoying"*.

Such system-enforced security demands are often experienced as a chore and can challenge users' ability to remember their passwords. Thus, we frequently identified posts in which people expressed their frustration about forgotten passwords. Expressions of anger or melancholy in this regard included: *"Omg I forgot my password to my fone!!!!!RS"*; or *"I wish I could change my Wi-Fi name, but apparently I don't have the correct password to do so. #sadface"*. Users also, albeit less often, tweeted about being relieved when they had regained access to an account: *"OMG I forgot you had my password. Wheeeww I thought I was going crazy [username]"*.

In some cases people also commented that losing or forgetting their passwords implied a loss in access to their online accounts as illustrated by these tweets: *"[username] I forgot my password 4 years ago, soooooo, I don't use that account anymore, Sherlock"*; or *"[username] I got a new twitter because I couldn't retrieve the password from my other one"*. While most online systems offer functionality for password retrieval, for some users this did not appear to be a possible solution or straight-forward process. Expressing frustration about difficulties to recover forgotten credentials, people tweeted for example: *"why is there no way for me to recover my skype name and password? gawddddd"*. Moreover, at times, available recovering options did not reflect the authentication problem that the user was facing: *"#ThatawkwardMoment when you can't remember your username, and the only option is "Forgot Password". #Why"*.

As a result, we identified a number of tweets in which users reported to have created a new account. However, specifically with regard to Twitter this comes at the cost of the person needing to reconstruct the list of people they were following and to re-contact their list of followers. Where the creation of a new account appeared to be the only possible course of action, this did not only feel frustrating to the account owner, but was also greeted by perplexion by others: *"Why do people make a new Twitter account when they forget their password instead of clicking the "Forgot Password button? #comeonpeople"*.

5.1.2 Password Management: Personal Practices & Workarounds

Difficulties related to the remembering of passwords described above led to descriptions of people abandoning existing accounts. Many users further admitted to have had the same password for many (if not all) of their accounts, undermining some of the security demands posed upon them: *"I Got The Same Password For Everythang!"*. Others openly described their approaches to recovering their passwords, explaining how they keep for example a record of these in their email account: *"[username] I can never remember the password LOL [laugh out loud]. I do have it saved in my mail though"*.

In addition to descriptions of such workarounds, people tweeted about how their remembering of certain passwords, especially online passwords, was complicated and addressed through the practices they had develop around their everyday password use (n = 150, 15%). Some described difficulties remembering their passwords due to routine, embodied typing mechanics: *"I barely remember my password, my fingers are just used to typing it so much"*. Again others explained how especially the automatized login processes on mobile devices that stores users' credentials can cause authentication problems when the user deletes certain mobile apps that hold their saved account details, or if they lose or change their devices. Describing these memorability problems users tweeted for example: *"I dont even know my password on twitter so if i ever lose my phone im f[?]d"*; *"[username] lol I know I forgot my twitter password so I can only tweet from one device where the password is saved"*; or *"[username] got anotha phone n dnt got my password to the account"*.

To gain general advice and support by others about how to recover one's passwords or manage hacked accounts, we found that users tweeted for example IT queries regarding Twitter to the official Twitter account: *"twitter won't let me login on my iPod. It used to but now it tells me "incorrect password or username" I've checked everything"*; or contacted the official support account: *"Support please fix the recaptcha thing it won't let me log in. im only able to log in if i reset my password"*. Moreover, users also frequently posted advice to each other about password management and privacy settings, and they warned one another about security breaches in relation to their accounts being hacked, providing advice how they could regain control. The following tweets illustrate this: *"[username] just go to your settings, go to password, change it, and then review who's on your account and you can revoke their access"*; or *"hi Mar, just to let u know that you may need to change your twitter password as i keep getting spam msgs from your account. Mark xx"*.

5.2 Social Practices around Passwords

A large proportion of the tweets that we analyzed (n = 306, 44%), described a wide range of social practices that evolved around the giving, receiving and resetting of a person's password. In the following we present examples of tweets that outline how the sharing of passwords has been a deliberate act in enabling access to certain resource for a specific individual or group of people; and in defining a relationship as close, intimate and trusting, or as doubtful and disappointing. Furthermore, the findings show how trying to guess the (online) password of a person in one's social network can become a playful social challenge rather than being perceived as a security threat; and how people who broadcast their passwords online do so under consideration as to how the target recipients would gain access to their devices or (online) accounts without compromising their overall security. All of these examples contribute to an experiential account of how passwords are embedded and have become of immense importance in peoples' daily and social lives, demonstrating how their role undoubtedly exceeds securing access to personal data.

5.2.1 Sharing Access to Resources with Social Network

We identified a number of tweets in our data set (n = 56,

8%) of users describing how they were sharing passwords as a way to manage and distribute access to resources such as WiFi or a person's Netflix account. For example, users tweeted to request or offer the password to certain online platforms for sharing the benefits and/or costs of a particular service with members of their social network: *"Getting my Netflix account back tomorrow..who wanna go half n get this password??"*; or *"If anyone wants to share with me their Netflix username and password I'll give you a prize (will be food)"*. Passwords were also shared with members of a specific social group to organize access to materials by these people. For example: *"just dm [direct message] me if you want the password to this account, ANYONE from the phandom can use it:)"*; or *"[username] can we recreate 6th grade and make a mom jean patrol club, only those with the password are allowed in"*.

5.2.2 Defining Relationships as Close and Intimate

Exploiting conventional assumptions that passwords are something to be kept private, several tweets (n = 52, 7%) described how people shared their passwords as a way of defining their relationship with friends, family members, or romantic partners. These tweets portrayed, at times playfully, how the giving, receiving, exchanging and possessing of access to someone's passwords reflected a certain closeness and intimacy between, and knowledge of, each other. For example, the following tweets indicate how, quite literally, the sharing and knowledge of a person's password with another person defined their relationship for example as 'romantic' or as 'friends': *"I cant call you my girl till you know my email password?"*; or *"[username] We're not friends until I have your wi-fi password"*.

Similarly, if a person was considered to be a romantic partner or friend, the sharing of their passwords appeared to be a social practice that was expected of them: *"If you don't give me your wifi password then we can't be friends anymore"*. However, this social obligation did not find acceptance by all, as is indicated in this tweet: *"idc [I don't care] if we date what you need the password to all my stuff for"*. Moreover, if the relationship had taken a hit or people fell out with each other, passwords were revoked: *"[username] I forgot the password on one and the other got blocked by [username] who I had an argument with :D xxx"*. In the context of exchanging passwords between people, we also found posts that reflected an adherence to the social norm of reciprocity, which was especially apparent in the following tweet: *"[username]... she has my password too... its equal"*.

Most striking however were expressions of closeness whereby the knowing of a person's password was equated with knowing the person: *"If you don't know my password than you don't know me"*. Equally, if a person had intimate knowledge of the other, they were better positioned to guess their passwords, as became apparent in the following two tweets: *"I'll give ya'll a hint. It's an 8 character password and the second letter is A"*; or *"my phone password is my crushes last name lol"*. This last tweet further indicates that choosing the names of people one is close to as passwords presents a frequent practice and one that can also cause difficulties, when the social bond is broken off, as this tweet demonstrates: *"And your name is still my password so I'm reminded of that shit everyday"*.

5.2.3 Giving and Revoking Trust to Others

In this context of password sharing, a number of tweets (n = 45, 6%) linked giving someone access to personal accounts or WiFi networks to an awarding of trust and the expectation that the recipient would treat the password appropriately (however socially defined in the different instances). Reminding the recipient of the responsibility that they had been given through the password, one user tweeted for example: *"Kaitlin's the only one that knows my password now. Sooo, I know it's you that just tweeted that Kaitlin"*.

The relationship between password sharing and trust, however, became most apparent in tweets where users openly expressed their disappointment and frustration about others 'abusing' their online accounts by deleting, changing or adding information. The following tweets illustrate this: *"Never give your password to sum1 else i learned from that cause they will delete your things"*; or *"i'm so paranoid i'm never giving anyone my password ever from now on oh my god"*. In response to the violation of trust that the password recipient had been given, Twitter users described to have revoked other peoples' access (e.g. by resetting their passwords): *"I'm not giving you the new wifi password next time you come home."*; or *"Gonna have to change my password so Casandra can't see these messages"*.

5.2.4 Playful Social Hacking

There have also been Twitter tweets describing peoples frustration and concerns about their accounts being struck by system hacking or phishing attacks (n = 36 as part of the password difficulties theme above). For example, a common observation were tweets to deceive users to disclose confidential information, such as: *"#retweet If you type your password on twitter, it shows up as stars! :D ******"*. However, we also identified various tweets (n = 87, 12%) where protecting one's password from known others (usually social connections/friends of the person) became an invitation and playful challenge for some to try 'guess', 'hack' or 'rape' their account. The following tweets exemplify such intents: *"What Breanna thinks my twitter password is?"*; *"If I had Josh's password I'd totally be raping his account right now. #StrangeUrges"*; or *"[username] Jon has my twitter password and conversates with himself"*.

To those who succeeded in guessing other peoples' passwords and hacking into their online accounts, this felt like an achievement, but we also found complaint tweets of those people who feel victim to such an attack: *"Ayeee, Boy Who hacked My Twitter I Will give Youu 24 Hours to Change My Damn name Back or My password Will Be changed"*.

5.2.5 Broadcasting Passwords: Physically and Socially Secured

Occasionally (n = 66, 9%), users also publicly posted their own or other peoples' passwords and pin codes on Twitter. However, those tweets may not have presented an immediate security threat, as they often required additional access to the device to which they would provide access. For example: *"Joes iPod password is 1337"*; or *"[username] Alright, I'm gonna leave my phone in here w/ you guys. My password's 0209 if you need it"*. Moreover, in tweets where uses requested a certain password of others, they often suggested a different channel for receiving it (e.g. send as a text message rather than a tweet). The following tweets illustrate this: *"[username] text me the password for raleys wifi"*; and *"[username] whats the WiFi password. Dm [direct message]*

it lol". In other words, only certain parts of an authentication process were publicly revealed that either required the person to be in reach of a particular password-protected device to complete access; to have sufficient 'knowledge' about that person (e.g. their home address to be able to make use of their WiFi credentials); or to qualify (e.g. as a 'close' friend) to be send a text message with the remaining details.

5.3 Use of Passwords and their Practices in Self-Portrayals

As a platform that invites the open sharing of personal opinions and thoughts, Twitter enables people not only to share information, but to communicate something about their self. Thus, we frequently observed how people used tweets and their understanding and (mis)uses of passwords to portray a particular image of their self (n = 155, 22%).

5.3.1 Raising Authenticity of One's Online Profile

A large proportion of those posts (textitn = 80, 11%) included messages of users admitting that they had forgotten their password or had trouble entering it correctly. About trying to remember their passwords and describing their difficulties to log into their accounts, users tweeted for example: *"Ok 12 year old self....what would you have made your password"*; *"I was typing the wrong password into Facebook #FacePalm"*; or *"Me: 'types in password, Password Doesn't Work' OMG I'M HACKED.... oh wait... never mind, CAPS LOCK WAS ON..' "*; and yet another user tweeted: *"[username] yeah but still trying to figure my password to my heathmax12 account. I swear I should be a natural blonde"*. While these tweets say very little about practical problems in relation to how people manage their passwords, they present expressions of malpractice with regard to how the person was handling certain difficulties. Such self-portrayals of inadequate behaviors however can raise the perceived authenticity of their online profile.

5.3.2 Insights into One's Security Attitudes and Practices

In contrast to tweets in which people present insufficiencies in how they manage their passwords, we also found a small proportion of tweets (n = 11, 2%) in which users presented themselves as concerned about protecting their passwords and keen to keep their accounts and devices secure. Most tweets in this regard included complaints about shoulder surfing attacks, and peoples' personal attitudes towards adding or regularly changing passwords. Examples include: *"I hate when people stare at the keyboard while I'm typing my password"*; *"I should really put a password on my phone."*; and *"Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months"*.

5.3.3 Presenting Oneself as Faithful, Cool or Funny

Some of the tweets (n = 27, 4%) with regard to peoples' portrayals of their identity further link to the previously described theme on 'trust', in that users related to their practices of password sharing as a means to describe themselves as faithful and to have nothing to hide. Users tweeted for example: *"I have nothing to hide he can have my password to everything including my phone. #faithful!"*; or *"?If I had a boyfriend, he'd know my password to my phone. I have nothing at all to hide"*.

In general, peoples' tweets would present a snapshot into their personality, presenting them for example as stubborn, unlucky, cool, and most commonly, as funny (n = 37, 5%). For example: *"I do have a life outside of Twitter, but I can't remember the password for it"*. Furthermore, some Twitter users specifically exploited the particular affordances and qualities of (online) passwords, their character composition and length, or the assumptions that people commonly have of them as something that should be kept private and secured from access by others in the telling of jokes. One user for instance tweeted the following: *"I was choosing a password for my new computer last night, I tried LiverpoolFC but apparently it was too weak"*; and another one posted: *"What's Forest Gump's password on Facebook? 1forest1. aha get it."*.

6. DISCUSSION

Over the past twenty years, digital technology and its associated security mechanisms have diffused into almost all aspects of people's lives which has considerable implications for how security technologies must be designed and studied [9]. After identifying social media as a potential resource of security-related experiences, we analyzed posts on the the example of the password due to its status as a security technology that has resisted a concerted research effort to find usable and secure alternatives [13]. The research we have conducted raises a number of discussion points around how studying personal experiences on social media sites can contribute to a better understanding of the design challenges facing security technologies;

6.1 Passwords as a Social Currency

Our main findings were around how passwords being appropriated as a social currency, where people were often thinking carefully about passwords and how the maximum value (both pragmatically and socially) could be derived from that password. We saw how the inherent value of passwords made them an item fit to be protected, shared or sought after in a social circle. The need to protect passwords was demonstrated in no small part through users' expressions of frustration at password loss (e.g. *"#sadface"*, *"#Annoying"*), and relief at rediscovery (e.g. *"Wheeeww I thought I was going crazy"*). The sharing of a password with another person can be a powerful act in defining a relationship (e.g. as trusting, as being close). Social expressions of trust were defined by the sharing of the password that regulated access to certain accounts or services, and were ended through the revoking and resetting of that password if a violation of this trust relationship occurred. This form of 'access control' is enabled through the affordances of passwords as they currently are. Twitter was often used to broadcast or discuss any violation of a trust relationship, and various memes that circulate in tweets shed light on how a person might like to respond in such circumstances.

Conventional wisdom considers that security is a secondary concern for users [30, 37]. This is typically true, however recent work has shown how passwords can be foregrounded in relationships where the sharing of credentials can serve functional purposes due to e.g. disability [8] or geographic isolation [32]. The trend of social hacking is particularly interesting, and is likely to be facilitated due to the increased user awareness of the limitations of password choice, but also the large number of opportunities that exist today to compromise passwords in some way. These activities are also less

likely to be interpreted as being deviant due to the lack of technical sophistication required to achieve such compromise e.g. displays are increasingly portable and high resolution, which permits shoulder surfing; devices can even be surreptitiously accessed shortly after a user has authenticated to a device; or people may forget to logout while checking emails on the device of a friend. Exploiting these situations can simultaneously provide friendly feedback that some security practices leave something to be desired, but creates a learning feedback of how accounts can be compromised in the social domain if that password are not appropriately managed.

Security researchers often design systems that must impede opportunities for users to perform certain actions. Traditional conceptions of passwords involved the assumption that they were strictly personal and not to be shared [23]. Our findings reinforce that technology designers should be mindful of the ways that people appropriate security mechanisms when designing systems that may aim to control behaviors; a goal that may contribute to the reduction rather than the increase of security.

6.2 Using Twitter for Understanding Security Experiences

The tweets we collected provided us with a snapshot into a wide range of very practical difficulties that people encounter in their daily routines around the use, set-up and maintenance of their passwords as well as a glimpse of their emotional responses. While in this paper we have focused upon tweets that concerned the use of passwords, it is likely that other areas of security and privacy are also discussed prominently on Twitter and could be studied in a similar way. The most suitable issues are likely to be those that are relatively common in everyday life, yet are ever-changing in how they manifest; for example: phishing [16], identity theft, email account hijacking [31], and computer viruses. Each of these areas has social engineering and deceit at its core, and studying tweets can likely provide a useful window to understand how users make sense of these attacks while they are underway, and how people might recover from them. Future research can verify whether this is the case.

An alternative approach to social media analysis could focus upon timely events in society that have privacy and security implications. Twitter was a particular hub of discussion during the recent heartbleed [4] controversy. Heartbleed was the name given to a bug discovered in the OpenSSL library that underpins much secure communication on the Internet. One piece of advice that emerged from this controversy was the need for users to change all of their passwords. At that time people turned to Twitter and used the hashtag #heartbleed extensively to complain about the possibility of changing passwords, and to seek more information from the crowd about the problem. This could lead to analyses of how attitudes to security and privacy change after significant events, or simply change naturally over time.

Recent work focused on security stories [29] and folk models [36] reinforce the need for a sustained focus on how people make sense of security technologies; it is possible that social media analysis can complement that research agenda and provide an accessible resource of stories for designers wishing to gather insights for technology design or simply understand existing behaviors better.

6.3 Challenges of using Twitter as a Research Method

Although tweets are restricted to only 140 characters in length and therefore require users to keep their statements brief, our analysis has shown how even short textual accounts provided insights into the practices and manifest experiences that people have with regard to passwords. Tweets however are limited in the extent to which they offer contextual background. Greater attention to capturing 'retweets' and 'replies' could alleviate this problem, but this issue mainly arises from the general absence of rich social cues online that are inherent to face-to-face rather than online mediated communication; this presented a challenge at times for the researchers to make sense of the tweets, some of which therefore had to be excluded from the qualitative analysis.

However, as intended for our present study, a manifest analysis of tweets provided us with a sense of the many pervasive and openly communicated (albeit often ignored in design and policy within the field) relational, social and personal factors that are at play and apparent in peoples' experiences of passwords. We regard this outcome as a first step, on which to build more in-depth and contextually richer future research. In this regard, Twitter itself may even become a useful vehicle to help identify potential research participants that have demonstrated through their public tweets certain interests or difficulties in a specific domain. Moreover, brief interviews could even be conducted via Twitter itself. Examples of this have been seen already from politicians (*#askboris* is a hashtag used by the Mayor of London to elicit questions from Londoners).

7. CONCLUSION

particularly where unusable and insecure passwords provide elements of social value. As security and privacy technologies increasingly penetrate most aspects of our lives, there is a need to develop research methods that provide a window into the ways that people appropriate security technologies into their everyday lives. It is particularly important to question the ways that security experts expect their technologies to be used, and contribute to the design of new, more experience-centred security mechanisms. In this paper we explored the use of social media as a window into everyday security practices. To do this we collected a large dataset of tweets on or related to #passwords. Our quantitative analysis suggests that Twitter is a platform for active discussion around password practices. Our findings shed light on contemporary password practices, and suggests that today, passwords can be considered a social currency that people seek to protect, share and obtain from others. These results have implications for our collective understanding of how people integrate passwords into their lives, and suggest Twitter as a platform where other learnings around security and privacy practices could be focused. Future work can consider how content from tweets can be source of design inspiration and feed into a process of experience-centred security and privacy design.

8. ACKNOWLEDGEMENTS

This work was supported by the RCUK Digital Economy Hub on Social Inclusion through the Digital Economy (SiDE) (EP/G066019/1).

9. REFERENCES

[1] About twitter. "https://about.twitter.com/company". Accessed: 2015-05-30.

[2] A. Bermingham and A. F. Smeaton. On using twitter to monitor political sentiment and predict election results. In *Workshop on Sentiment Analysis where AI meets Psychology (SAAIP)*, 2011.

[3] W. E. Burr, D. F. Dodson, and W. T. Polk. *Electronic authentication guideline*. Citeseer, 2004.

[4] M. Carvalho, J. DeMott, R. Ford, and D. A. Wheeler. Heartbleed 101. *Security & Privacy, IEEE*, 12(4):63–67, 2014.

[5] M. Doughty, S. Lawson, C. Linehan, D. Rowland, and L. Bennett. Disinhibited abuse of othered communities by second-screening audiences. In *Proceedings of the 2014 ACM international conference on Interactive experiences for TV and online video*, pages 55–62. ACM, 2014.

[6] P. Dourish and K. Anderson. Collective information practice: emploring privacy and security as social and cultural phenomena. *Human-computer interaction*, 21(3):319–342, 2006.

[7] M. Duggan and A. Smith. Social media update 2013. *Pew Internet and American Life Project*, 2013.

[8] P. Dunphy, A. Monk, J. Vines, M. Blythe, and P. Olivier. Designing for spontaneous and secure delegation in digital payments. *Interacting with Computers*, page iwt038, 2013.

[9] P. Dunphy, J. Vines, L. Coles-Kemp, R. Clarke, V. Vlachokyriakos, P. Wright, J. McCarthy, and P. Olivier. Understanding the experience-centeredness of security and privacy technologies. In *Proc. of the New Security Paradigms Workshop (NSPW)*, 2014.

[10] B. G. Glaser and A. L. Strauss. *The discovery of grounded theory: Strategies for qualitative research*. Transaction Publishers, 2009.

[11] S. A. Golder and M. W. Macy. Diurnal and seasonal mood vary with work, sleep, and daylength across diverse cultures. *Science*, 333(6051):1878–1881, 2011.

[12] G. R. Hayes. The relationship of action research to human-computer interaction. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 18(3):15, 2011.

[13] C. Herley and P. Van Oorschot. A research agenda acknowledging the persistence of passwords. *Security & Privacy, IEEE*, 10(1):28–36, 2012.

[14] Y. Hwang. Antecedents of interpersonal communication motives on twitter: Loneliness and life satisfaction. *International Journal of Cyber Society and Education*, 7(1):49–70, 2014.

[15] P. G. Inglesant and M. A. Sasse. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 383–392. ACM, 2010.

[16] M. Jakobsson and S. Myers. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons, 2006.

[17] A. Java, X. Song, T. Finin, and B. Tseng. Why we twitter: understanding microblogging usage and communities. In *Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 workshop on Web mining and social network analysis*, pages 56–65. ACM, 2007.

[18] J. Kaye. Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2619–2622. ACM, 2011.

[19] D. V. Klein. Foiling the cracker: A survey of, and improvements to, password security. In *Proceedings of the 2nd USENIX Security Workshop*, pages 5–14, 1990.

[20] A. D. Kramer. An unobtrusive behavioral model of gross national happiness. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 287–290. ACM, 2010.

[21] K. Krippendorff. *Content analysis: An introduction to its methodology*. Sage, 2012.

[22] V. Lampos and N. Cristianini. Tracking the flu pandemic by monitoring the social web. In *Cognitive Information Processing (CIP), 2010 2nd International Workshop on*, pages 411–416. IEEE, 2010.

[23] S. Mandujano and R. Soto. Deterring password sharing: User authentication via fuzzy c-means clustering applied to keystroke biometric data. In *Computer Science, 2004. ENC 2004. Proceedings of the Fifth Mexican International Conference in*, pages 181–187. IEEE, 2004.

[24] J. McCarthy and P. Wright. Technology as experience. *interactions*, 11(5):42–43, 2004.

[25] J. McCarthy and P. Wright. Putting âĂŸfelt-lifeâĂŹat the centre of human–computer interaction (hci). *Cognition, Technology & Work*, 7(4):262–271, 2005.

[26] M. R. Morris, S. Counts, A. Roseway, A. Hoff, and J. Schwarz. Tweeting is believing?: understanding microblog credibility perceptions. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, pages 441–450. ACM, 2012.

[27] D. A. Norman. *Emotional design: Why we love (or hate) everyday things*. Basic books, 2004.

[28] M. J. Piskorski. *A Social Strategy: How We Profit from Social Media*. Princeton University Press, 2014.

[29] E. Rader, R. Wash, and B. Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 6. ACM, 2012.

[30] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the âĂŸweakest linkâĂŹâĂŤa human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3):122–131, 2001.

[31] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo. My religious aunt asked why i was trying to sell her viagra: experiences with account hijacking. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 2657–2666. ACM, 2014.

[32] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 895–904. ACM, 2007.

[33] A. Smith and J. Brenner. Twitter use 2012. *Pew Internet & American Life Project*, page 4, 2012.

[34] M. Thelwall, K. Buckley, G. Paltoglou, D. Cai, and

A. Kappas. Sentiment strength detection in short informal text. *Journal of the American Society for Information Science and Technology*, 61(12):2544–2558, 2010.

[35] A. Tumasjan, T. O. Sprenger, P. G. Sandner, and I. M. Welpe. Election forecasts with twitter: How 140 characters reflect the political landscape. *Social Science Computer Review*, page 0894439310386557, 2010.

[36] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[37] A. Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Usenix Security*, volume 1999, 1999.

[38] P. Wright and J. McCarthy. Empathy and experience in hci. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 637–646. ACM, 2008.

[39] P. Wright and J. McCarthy. Experience-centered design: designers, users, and communities in dialogue. *Synthesis Lectures on Human-Centered Informatics*, 3(1):1–123, 2010.

[40] M. E. Zurko and R. T. Simon. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms*, pages 27–33. ACM, 1996.