Fifty shades of grey hat: A socio-psychological analysis of conversations on hacking forums

John McAlaney [a], *Emily Kimpton* [a] *and Helen Thackray* [b]
[a] *Bournemouth University*
[b] *University of Portsmouth*

Abstract. There remains a lack of understanding as to what determines the path which a young person takes when they first engage with computers and hacking. This research sought to address that gap by exploring the conversations that take place on hacking forums and subreddits. Text in hacking related threads was collected from these sites over the summer period of 2018. Linguistic Inquiry and Word Count (LIWC) software was used to determine the linguistic characteristics of each forum/ subreddit. Thematic analysis was then conducted on a sub-set of text from each source. The results of the LIWC analysis indicated that there are variations in several psychologically relevant factors between these forums and subreddits, including the degree to which users used language that indicated they were being honest, confident, analytical and emotional. There were several results that were inconsistent with stereotypes of hackers, such as a relative absence of language indicating anger. The thematic analysis identified several themes relating to knowledge, skills acquisition, honesty legality and risk. Overall this research demonstrates that there exists an established online community of hackers, which are likely to be encountered by any young person who becomes interested in cybersecurity and hacking. These communities may potentially act as an important source of social support and social identity for their members. Understanding the dynamics of these communities may better help us steer people towards legitimate cybersecurity careers, where their passion and skills can be used for societal good.

Keywords.

1. Introduction

The cybersecurity industry is experiencing a recruitment crisis [1]. There is a lack of people with the necessary skills applying for cybersecurity positions. Yet there are multiple online and offline communities composed of individuals with an interest in cybersecurity who potentially have the skills and knowledge necessary to fill these gaps. Such individuals are often identified as hackers. This is a term that have several negative connotations, and one which we have found in our own research is viewed as problematic by those who may be externally labelled as hackers [2]. These stereotypes mask the nuances and complexities of groups and individuals with an interest in hacking who, although they may wish to identify weaknesses in systems, have no desire to exploit these for criminal gain [3]. Of course, there are hackers who have criminal and malicious intent, but it important to understand the wider context. It has been observed that types and motivations of hacking are varied and complex [4], although such models are often based on case studies or media reports of hacking incidents. This lack of studies that use data directly from people who identify has hackers may reflect the perceived difficult of engaging with this particular population [3].

Given these negative associations with hacking, coupled with the innate interest in computing, it is unsurprising that many individuals undertaking hacking choose to participate in online hacking forums. As has been found in other areas such forums can provide a social context for individuals [5], and become an important source of self-esteem and social identity [6]. In order to map how people's interest in hacking manifests it is important to engage with and better understand these communities. By doing so it may be possible to identify risk factors that are associated with individuals becoming involved in criminal hacking. It may also enable us to better empower individuals to pursue legitimate careers in cybersecurity.

One method that can be used to help understand the psychological characteristics of an online group is the analysis of the language used within that group [7]. This approach has been used to explore group dynamics, social processes and emotions within other online communities including those relating to mental health [8] and recovery from alcohol use [9]. However, many of these studies focus on health behaviours or in some form of behaviour change overall. From our research it is evident that people who engage in hacking do not see this as a problematic behaviour which needs to be fixed – as noted by several participants in our previous studies hacker does not equal criminal [2]. There may also be unique characteristics to hacking forums that alter how such discussions take place, compared to forums for other behaviours. It has been noted for example that support groups are characterised by high levels of reciprocal self-disclosure [10], although it may be that this phenomenon will be less prevalent in discussion on hacking forums, given the perceived risk of becoming the focus of law enforcement.

The study reported here is part of ongoing, exploratory work to determine how different methodologies can be used to analyse the discussions held on forums relating to hacking. In doing it contributes towards this under-researched but increasingly socially and economically important topic

2. Method

Data was collected from online forums and subreddits (from the Reddit website) related to hacking. An initial list of potentially relevant forums and subreddits (henceforth collectively referred to as 'sites') was created based on the previous experience of the authors in this area, which included interviews with people who identify as hackers and attendance at hacking events, including the DEFCON event held annually in Las Vegas [2]. Each of these sites was then evaluated by the authors to determine if there was sufficiently substantive content relating to hacking to merit an analysis of that site. A total of four hacking forums and three subreddits were selected for the purposes of this study. The approach to the selection and analysis of the sites was informed by web forum analysis guide provided by Holtz et al [11].

The authors then began the process of exporting text from the sites into Word documents. Discussion threads were selected based on if they included substantive discussion on the topic of hacking; given that within each site there were threads that related to non-hacking issues. Examples of the threads that were used in the analysis include; 'How to crack Instagram accounts?'; 'Made this tool for newbies'; 'Need lessons'; 'a skid, a hacker, or just damm lazy?'; 'credit card fraud'; 'Am I wrong that hacking is better off self-taught?'; 'My computer was hacked – how?' and 'Where can leaked password lists be found?'. Approximately 120,000 words of text were collected from across all of the sites.

Analysis of the text was done using the Linguistic Inquiry and Word Count (LIWC) software [12]. This software identifies the frequency of words within a text source and from this derives linguistic categories, including psychological processes. It has been used within multiple studies to explore personality [13], stress reactions to events [14] and social psychologically related processes such as deception [15]. It has also been used in previous studies specifically for the analysis of discussions held within subreddits of Reddit [8].

LIWC produces results for a high number of categories. This includes four summary variables which are generated for each piece of text, which are named analytical thinking, clout, authenticity and emotional tone. Each of these is scored 0 – 100, with a higher score indicating greater presence of that variable within the text. Analytical thinking reflects the degree to which individuals demonstrate formal, logical and hierarchical thinking patterns [16]. Clout is a measure of the relative social status, confidence and leadership that individuals display through their writing [17]. Authenticity measures the degree to which people are using language that indicates they are being more personal, honest and vulnerable [18]. Finally, emotional tone indicates the degree to which positive and negative emotions are evident in the text, with a score below 50 suggesting a more negative emotional tone [14]. In addition, the software generates 21 standard categories (percentage of pronouns, auxiliary verbs, etc.) and 41 semantic categories of psychological constructs (e.g. affect, cognition, inhibition, achievement). For the purposes of this study 4 semantic categories were included in the analysis, which were chosen based on the literature. These were Social, Power, Risk and Anger.

Following the LIWC analysis a thematic analysis was conducted on a sub-set of each text file, using the Braun and Clarke method [19]. This analytical approach was chosen due to exploratory nature of the study and the lack of a strong theoretical basis underpinning this topic. A selection of approximately 3000 words of text was analyzed from each site. Coding was conducted on each sample of text independently by two of the authors. Themes were then generated, reviewed, refined and named by the lead author.

Ethical approval for the study was obtained through the relevant institutional ethics committee.

3. Results

3.1 LIWC analysis

There was some notable variation in the LIWC scores on the four summary variables, as shown in Table 1. Several forums displayed a lower score on analytical thinking than the others, with subreddits overall demonstrating greater levels of analytical thinking than web forums. Similarly, there were variations in the clout score between sites, indicating differences in the ways in which confidence, social status and leadership is expressed within those sites. Authenticity scores was markedly higher on some sites than others

	Word count	Analytic	Clout	Authentic	Tone
Forum 1	8595	33.1	55.59	43.84	51.92
Forum 2	11112	41.73	62.34	52.85	62.96
Forum 3	24986	47.98	52.9	44.7	45.7
Forum 4	19014	54.4	59.89	29.97	44.03
Subreddit 1	14116	54.78	60.41	47.9	55.84
Subreddit 2	25104	53.18	56.78	31.41	58.78
Subreddit 3	15687	51.98	64.98	31.14	47.97

Table 1. Word count and LIWC score on analytical thinking, clout, authenticity and emotional tone.

The results for the 4 chosen semantic categories of psychological constructs are shown in Table 2. The variation between sites was relatively small. Approximately 10% of the language used in the sites related to social factors. Similarly, power related words were relatively consistently used across sites. Both language relating to risk and anger were rarely used within sites.

	Social	Power	Risk	Anger
Forum 1	10.24	2.28	0.9	0.79
Forum 2	10.42	2.5	0.61	0.86
Forum 3	8.14	2.13	0.68	0.48
Forum 4	9.1	2.86	0.69	1.05
Subreddit 1	10.25	1.88	0.45	0.73
Subreddit 2	8.01	2.34	0.64	0.58
Subreddit 3	9.12	2.49	1.08	0.64

Table 2. LIWC scores on selected categories.

3.2 Thematic analysis

Several themes were identified through the analysis, as summarized below.

Skill acquisition: A common theme across all sites was the desire to learn new skills relating to programing and hacking. As part of this there was a perception that hackers were often self-taught, although there was also an acknowledgement that formal training could be useful. Regardless of the route through which individuals acquired hacking skills there was a strong sense of people needing to have an underlying passion for the topic if they were going to succeed in becoming a hacker or cybersecurity professional.

'As far as self-taught vs otherwise, the difference in this field is passion. People who are self-taught are that way because they have passion for it, and that leads to them becoming smart/successful'

As part of this users were directed to seek out support and trusted others who they could discuss and practice hacking techniques with.

'It is about finding someone or a group of someones that you can trust enough to bounce ideas off of and learn new techniques, a lot of what you would call hacking can be learned right from google. What you need to do is network and find friends that you can "test" on and also learn from, maybe have a little hacker war. Be cautious on who you trust though'[sic]

Whilst there appeared to be a degree of respect for individuals who were attempting to learn hacking on their own it was also evident that there were high expectations for them to do so properly with, on some occasions, members of the forum displaying low tolerance for new members who were perceived to made an inaccurate comment or to have asked a foolish question.

'If you didn't know when unhashing process stops some passwords don't get recovered, so it wouldn't match every right password! YOU ARE A SUCH A NOOB!' [sic]

Legality: Discussions on all sites frequently referred to the legality of different actions. A typical scenario would be a user posting a request for information on how to do an illegal activity (for accessing a social media account). Whilst some practical advice might be offered in response to these questions most responses would instead point out to the user that what they are requesting is illegal, often with a further criticism that the users appeared to have a stereotypical view of what hacking is.

'ahh my friend, u miss understand the term "hacking" , hacking does not mean illegal infilrattion of the DOD or watever shit like that, hacking is much more then taht, its makeing the most out of what you have and making it it work for u' [sic]

A frequent occurrence was for users to disclose that they had already taken part in an illegal activity and had received some form of warning message from the targeted organization/ service provider stating that they had been identified. The responses to such posts varied extensively, from those which advised that it was unlikely further action would be taken for relatively minor breaches (often phrased in a sarcastic way), to those which instructed the user to take steps to protect themselves. However, given the extensive use of trolling throughout these websites it was on some occasions difficult to determine how serious the intention was behind the advice.

Risk: Another theme was that of risk, and how acceptable different levels of risk were. There was also discussion on how to mitigate these risks. These comments were often linked to the theme of Legality, with what could be described as a cost-benefit analysis taking place in which the degree of risk was discussed in relation to the possible legal consequences if the person was caught.

'Can anyone confirm is this is too risky now? I think I might take a break from it now'

Honesty: Users were frequently challenged on the veracity of their identity and post content. Users were questioned on posts related to claims that they had been arrested over an activity, or that an online resource used by hackers had become compromised by law enforcement. Multiple reasons were given by those making the challenge on why the user appeared to be presenting a false narrative, including a suggestion that it was an attempt to drive business towards the original poster. This relates to hackers selling their services online [20].

*'Can you ban @****? he is lying and trying to scare everyone to get more clients for himself'*

Knowledge: It was evident that knowledge is an important factor in the identity of both the groups and the users. Individuals distinguished themselves based on their knowledge of hacking, with a degree of disdain evident towards those who rely on software they obtain online that does much of the hacking for them (known as a script kiddie, skiddie or skid).

'The information could be biased or plain incorrect, of course not bashing everybody who teaches hacking but simply put a very high percentage of people here don't know a dime about hacking'

Despite this it appeared that individuals who demonstrated a degree of self-awareness about the limits of their own knowledge would sometimes receive a less aggressive response, along with recognition that the use of online hacking tools was an increasingly common starting point for those entering hacking.

'I'm a lot more antagonistic towards script kiddies than I should be, but your eagerness and drive is what will make you guys the next cybersecurity professionals to take over the field'

4. Discussion

It is interesting to note both the differences and similarities in the language used between sites. Analytical thought was more evident overall on the subreddits than on the web forums. This may reflect a different style of interaction on Reddit, as opposed to more traditional web forums. It could be argued that nature of posts on Reddit are more transient, with popular posts and responses upvoted, resulting in a higher degree of visibility. This may encourage individuals to focus on conveying their arguments in a precise and more logical way, as they have a limited window in which to present their stance to the audience. Overall the language used within each site demonstrated a reasonably high level of clout, indicating that users were demonstrating confidence, social status and leadership in their posts and replies. This is consistent with the thematic analysis, that identified knowledge as a theme that is important amongst the users of these sites, and indeed perhaps even the key identifier of where individuals stand within the hierarchy of the group. This is also consistent with proposed typologies of hackers, such as Seebruck's model [4] that identifies prestige an a motivation for hacking. This is an important point. Prevention and mitigation strategies within cybersecurity could be argued to adopt Protection Motivation Theory, in which an individual decides whether to engage in a risky behaviour based on how severe they think the consequences may be and how likely this consequence is to happen [21]. In the case of hackers an organization may for example attempt to dissuade potential hacking attempts be presenting themselves as having such good defenses as to be impregnable, with attempts to breach their systems inevitably resulting in the attacker being identified and prosecuted. For hackers who are motivated in gaining prestige and social status such an approach by an organization may in fact increase their desire to breach that organization, as in doing so they obtain bragging rights as being one of the few people able to do so. This factor may also be relevant in situations where hacking groups are challenged on their abilities. A successfully implemented cybersecurity attack involving the hacktivist collection Anonymous for instance appeared to be largely triggered by a technology security company publicly implying that their skills were greater than that of Anonymous [6].

Authenticity also varied between sites, to a greater degree than was expected. Participation in hacking forum discussions is not of course in itself illegal, and as noted many posts explicitly condone any illegal activity. Nevertheless, it was assumed that the nature of the sites would result in individuals being consistently less honest and displaying less vulnerability across all the sites. On the other hand, it could be assumed that most users of the website had taken at least basic steps to protect their offline identity, by using pseudonyms and by not sharing information that could be identify them. If so then it is possible such users feel freer to be open and honest about their opinions and experiences. As has been noted in social psychological research anonymity within online groups can result in a stronger sense of communal identity than those where members know the identity of each other [22]. The degree to which members display authenticity within the sites may also reflect the social norms that have developed within that site. It is known that individuals will tend to alter their behaviour and cognitions to match the group to which they perceive themselves to belong [23], and yet at the same time tend to underestimate how much they influenced by the group [24]. It was noted that there several instances throughout the text where individuals referred to one of the other sites, typically in a disparaging way, and commented on that people who posted on that site were of a certainty personality type or skill level. This may indicate that individual use a small number of sites exclusively and with a degree of loyalty, although given the tendency of some users to conceal their identity it is difficult to determine if the same individual is active on

more than one site. Regardless of whether users were being honest or not there appeared to be, as revealed in the thematic analysis, an underlying feeling that anyone on the site could be lying and that nothing should be assumed to be true.

Authenticity may also relate to the emotional tone of the discussions on the site, which again varied between sites. As based on the LIWC scores some sites appeared to be characterized by an overall positive emotional tone, whereas other were overall slightly negative. It has been found emotions can spread amongst a group [25], which may reinforce social norms within that group in terms of what topics are discussed and what is considered appropriate. There was though relatively infrequent use of language that indicated anger. This contrasts with the popular stereotype of hackers that includes , perhaps best exemplified by an infamous Fox News report that described the Anonymous as an 'Internet hate machine' [6]. It should be noted that a degree of caution must be used when assessing the use of aggressive or emotional language in relation to discussions on hacking forums. As Coleman observes the style of interaction on many sites can, on the surface, appear to be quite markedly aggressive, sarcastic and confrontational [6]. This does not mean however that the individuals using this language do feel hostile towards one another. Instead it may simply reflect how users of these forums have come to communicate.

An important part of many of the posts was the theme of skills acquisition. This was often intermingled with the topic of risk, in terms how to learn or practice a skill without the individual putting themselves at risk of being arrested. It was also closely linked to the aforementioned theme of knowledge, where individuals who had experience would provide advice now how to perform an action or, as was often the case, why someone should not even attempt to perform an action at all on the basis of the high risk this would involve. This advice was not always provided freely. Responses to requests for advice or information were often met with aggressive or sarcastic answers. An important factor in determining whether a positive response was provided or not appeared to be the perceived authenticity of person seeking advice, and if they had appeared to have made a genuine to find the answer themselves.

Linked to risk and skills acquisition was the theme of legality. This was a constant topic through many of the threads. There were instances were illegal behavior was discussed and where advice was given to support illegal actions, but most threads clearly condoned illegal activities. This is consistent with out previous research that found that only a minority of people who engage in hacking believe that weaknesses and flaws in systems should be exploited [3]. The same research though did also find that most of such individuals believed that flaws and weaknesses in systems should be exposed. This especially appears to the case when the organization in question has enough resources for it to be reasonable to feel that they should not have such gaps in the first place. This may create some grey areas, where it is debatable if accessing a system to highlight the flaws it has to the owners of that system is illegal.

It is acknowledged that there is likely a degree of selection bias in the choice of threads from each site. The data collected is only a snapshot from a specific time point. In addition, it should be noted that the style of writing used in online forums and subreddits does tend to have greater levels of spelling errors, abbreviations and jargon than may be the case for other text sources. This may have created some issues with how closely the LIWC software was able to match the text to the inbuilt dictionary that it uses. Finally, the analysis was restricted to those posts that were in the English language.

Overall there are several active online communities where discussions about hacking take place. There is a lack of research on the pathways through which people, especially young adults, become involved in hacking but it would seem reasonable to assume that at least some of them will encounter these online forums when they first become interested in hacking. This study demonstrates that the discussions within these online communities can be studied in order to better understand how individuals may be influenced in their hacking behaviors and beliefs. It also shows that there exists a substantial knowledge base of hacking that could potentially be drawn upon to help address the serious challenges society is facing around cybersecurity and the lack of qualified professionals. By engaging with these communities, it may be possible to steer young adults away from activities that will result in them receiving a criminal record, and towards the growing number of unfilled, legitimate cybersecurity job vacancies.

References

1. Olenick, D. *Cybersecurity job gap grows to 3 million*. 2018 29/4/19]; Available from: https://www.scmagazine.com/home/security-news/cybersecurity-job-gap-grows-to-3-million-report/.
2. Thackray, H., *Hackers gonna hack: Investigating the effect of group processes and social identities within online hacking communities*, in *Psychology* 2019, Bournemouth University: Poole.
3. Thackray, H., et al., *Surveying the hackers: The challenges of data collection from a secluded community* in *16th European Conference on Cyber Warfare and Security*. 2017: Dublin.
4. Seebruck, R., *A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.* Digital Investigation, 2015. **14**: p. 36-45.

5. Liu, Y., et al., *When support is needed: Social support solicitation and provision in an online alcohol use disorder forum.* DIGITAL HEALTH, 2017. **3**: p. 2055207617704274.
6. Coleman, G., *Hacker, Hoaxer, Whistleblower, Spy : The Many Faces Of Anonymous*. 2014, London: Verso.
7. Pennebaker, J.W. and T.C. Lay, *Language use and personality during crises: Analyses of Mayor Rudolph Giuliani's press conferences.* Journal of Research in Personality, 2002. **36**(3): p. 271-282.
8. Lyons, M., N.D. Aksayli, and G. Brewer, *Mental distress and language use: Linguistic analysis of discussion forum posts.* Computers in Human Behavior, 2018. **87**: p. 207-211.
9. Kornfield, R., et al., *What do you say before you relapse? How language use in a peer-to-peer online discussion forum predicts risky drinking among those in recovery.* Health Commun, 2018. **33**(9): p. 1184-1193.
10. Barak, A. and J.M. Grohol, *Current and future trends in Internet-supported mental health interventions.* Journal of Technology in Human Services, 2011. **29**(3): p. 155-196.
11. Holtz, P., N. Kronberger, and W. Wagner, *Analyzing internet forums: A practical guide.* Journal of Media Psychology: Theories, Methods, and Applications, 2012. **24**(2): p. 55-66.
12. Pennebaker, J.W., et al., *The development and psychometric properties of LIWC2015*. 2015, University of Texas at Austin: Austin, TX.
13. Pennebaker, J.W. and L.A. King, *Linguistic styles: Language use as an individual difference.* Journal of Personality and Social Psychology, 1999. **77**(6): p. 1296-1312.
14. Cohn, M.A., M.R. Mehl, and J.W. Pennebaker, *Linguistic markers of psychological change surrounding September 11, 2001.* Psychol Sci, 2004. **15**(10): p. 687-93.
15. Toma, C.L. and J.T. Hancock, *What lies beneath: The linguistic traces of deception in online dating profiles.* Journal of Communication, 2012. **62**(1): p. 78-97.
16. Pennebaker, J.W., et al., *When small words foretell academic success: The case of college admissions essays.* Plos One, 2014. **9**(12).
17. Kacewicz, E., et al., *Pronoun use reflects standings in social hierarchies.* Journal of Language and Social Psychology, 2014. **33**(2): p. 125-143.
18. Newman, M.L., et al., *Lying words: Predicting deception from linguistic styles.* Personality and Social Psychology Bulletin, 2003. **29**(5): p. 665-675.
19. Braun, V. and V. Clarke, *Using thematic analysis in psychology.* Qualitative Research in Psychology, 2006. **3**: p. 77 - 101.
20. McCamy, L., *7 things you can hire a hacker to do and how much it will (generally) cost*, in *Business Insider*. 2018.
21. Rogers, R.W., *A protection motivation theory of fear appeals and attitude change.* Journal of Psychology, 1975. **91**(1): p. 93.
22. Tanis, M. and T. Postmes, *A social identity approach to trust: interpersonal perception, group membership and trusting behaviour.* European Journal of Social Psychology, 2005. **35**(3): p. 413-424.
23. Kelman, H.C., *Interests, relationships, identities: Three central issues for individuals and groups in negotiating their social environment.* Annual Review of Psychology, 2006. **57**: p. 1-26.
24. Darley, J.M., *Social organization for the production of evil.* Psychological Inquiry, 1992. **3**(2): p. 199-218.
25. Smith, E.R., C.R. Seger, and D.A. Mackie, *Can emotions be truly group level? evidence regarding four conceptual criteria.* Journal of Personality and Social Psychology, 2007. **93**(3): p. 431-446.