# Malicious Twitter Usage: Repurposing Accounts

Navi Boyalakuntla
*Stanford University*

Manda Tran
*Stanford University*

## Abstract

Twitter bans account transfers explicitly, but largely fails to enforce this type of malicious behavior. Account transfers are difficult to track, but the repurposing of accounts is not. This paper aims to characterize and investigate the behaviors of repurposed accounts. We (1) describe features and types of repurposed accounts and (2) provide recommendations to the Twitter legal team regarding language around account repurposing and how enforceable account transfers are in practice. We find that repurposed accounts *can* be identified using longitudinal data and leveraging differences between profile identity attributes like username, screen name, and biographical information. Additionally, we identify gaps in Twitter's current policies and describe methods to prevent repurposed accounts in the future.

## 1 Introduction

Twitter, a major social media and microblogging platform, provides monetization incentives for accounts with large influence either through Twitter directly or through external brand deals and affiliate links [6, 11]. However, these opportunities give rise to malicious marketplaces to buy and sell accounts, followers, and engagement for those who seek monetary gain.

Previous work has explored the intricacies of these marketplaces, generating models for detection and characterization of bot-like activity associating with spam and phishing. This usually involves tracking major changes like follower counts or the detection of bot-like activity. The goal of our paper is to detect a more subtle, yet equally misleading activity on Twitter, the repurposing of accounts. A *repurposed account* is an account that drastically shifts its content focus yet maintains the original following with an attempt to conceal its original identity. There are many different reasons why someone might repurpose an account on Twitter including malware, promoting their business with the previous account's influence, phishing scams, etc. We further define repurposed accounts in Section 3.1 and discuss how repurposing evades Twitter's current policy, yet can replicate the same malicious behavior buying and selling followers exhibits.

It can be seen in Figure 1 that it is difficult to enforce account sales and transfer rules on Twitter; it can be impossible to confirm with reasonable certainty that a different person is operating an account. In this paper, we explore an identifiable drastic account change that is currently still allowed under the platform manipulation and spam policy. We also make an important distinction between a *repurposed account* (which isn't in violation of Twitter policy) as an account displaying a drastic change in content, but not necessarily the person operating the account and a *transferred account* (which is in violation of Twitter policy) as a change in the person operating the account, but not necessarily the content.

We argue that account repurposing is more identifiable than account transfers and is malicious in most cases as it misleads the follower base and Twitter user space at large. In this paper, we use longitudinal data to better understand Twitter account repurposing in practice. We additionally provide recommendations to the Twitter legal team to add language around account repurposing and how enforceable account transfers have been in practice. In our paper, we aim to highlight the extent to which repurposed accounts are malicious to inform Twitter policy to prevent repurposed accounts in the future.

We find and define different classes of repurposing on Twitter. To do so we defined two major classes of accounts, *personal accounts* and *non-personal accounts*. Personal accounts are involve content directly related to an individual. Non-personal accounts include content for organizations, businesses, or certain topics of interest (i.e., fitness motivation, cooking, pets) that are not associated with or clearly run by a particular person. We find accounts that change from (1) non-personal accounts to a distinctly different non-personal accounts, (2) personal accounts to non-personal accounts or vice versa, and (3) personal accounts to a distinctly different personal account. In characterizing these repurposed accounts we identify, through existing literature and our own observations, possible steps to repurpose an account include changing

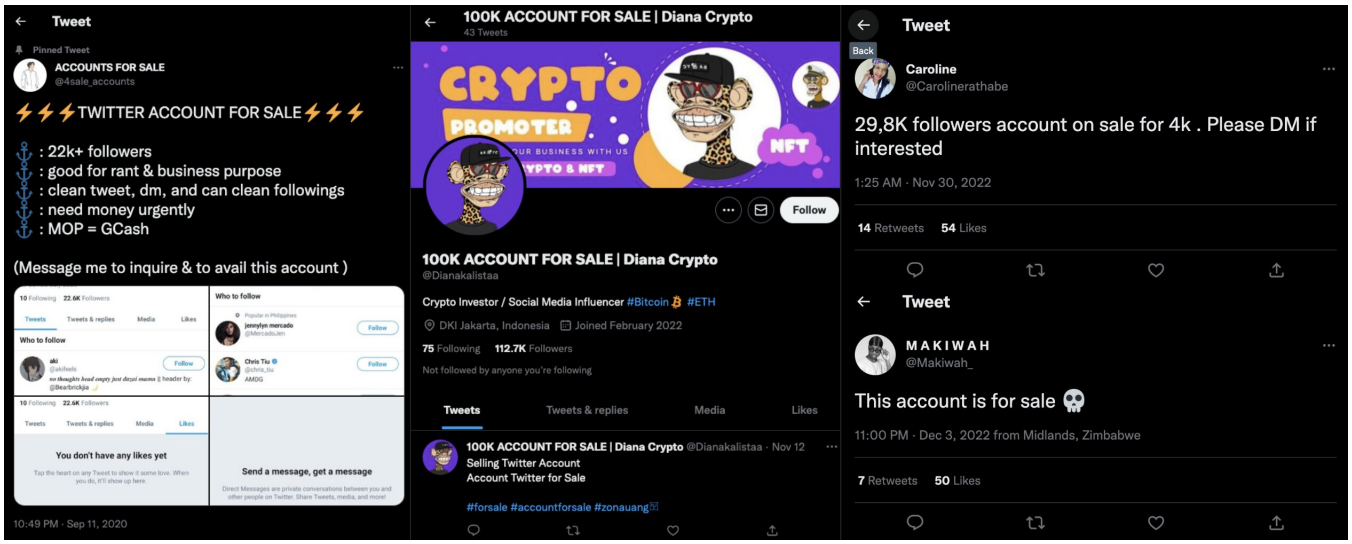


Figure 1: Evidence of prohibited account sales and transfers on Twitter found via the search utility on the Twitter platform.

the profile information, the username, and replacing old and irrelevant content with new content. We additionally explore three cases of clearly repurposed accounts in-depth.

In Section 2, related work in the space of identifying malicious behavior on social media is outlined. Section 3 details the methodology we used to prove the existence of repurposed accounts on Twitter. Section 4 summarizes the results from the identification of repurposed accounts. Section 5 includes three case studies of accounts that are clearly repurposed. Section 6 lists proposed policy changes to Twitter based on repurposed account identification. Lastly, Section 7 concludes the paper with a brief discussion.

## 2 Related Work

There has been an increased effort to better understand the malicious usage of social media platforms in several specific areas.

**Compromised Accounts** A vast majority of the existing literature describing compromised accounts illustrate attackers exploiting compromised accounts by using a previous trusted account, for spam or phishing. The behavior of users whose Twitter accounts were compromised was classified by Zangerle E., and Specht, G [13]. Gao, H., et al. developed a system to detect malicious Facebook wall posts [3]. Grier, C., et al. also worked to characterize spam on Twitter and better understand what makes Twitter spam successful [4].

Stringhini et al. investigated how adversaries convince Twitter users to compromise their credentials and find accounts that buy followers using the following list of compromised accounts. The authors analyze the victim's behavior to quantify the number of Tweets promoting these underground markets and gain an estimate of the number of victims [8]. This paper differs to research involving *compromised accounts* in that it studies account repurposing. Repurposed accounts are largely different from compromised accounts in that they aim to take advantage of the account's influence without the awareness of subscribed followers. Often, compromised accounts don't make an attempt erase the account's previous presence. Additionally, compromising an account is almost always an attack on the previous owner, while repurposing an account is not. However, as Stringhini G., et al. states, account influence is inextricably linked to compromised accounts which is highly relevant to the repurposing of accounts [8].

**Purchased Accounts** The existence of account-selling websites and social media posts like EpicNPC.com or playerup.com illustrate a marketplace for account sales and transfers. Recent work has analyzed account sales on Youtube for monetization exploits, but in general exposes a marketplace for selling accounts across many different social media platforms [1]. Thomas, K., et al. build a classifier that can identify fraudulent accounts sold via the underground marketplace [9]. they infiltrated this underground market to better understand its function.

**Repurposed Accounts** Account repurposing can occur willingly (e.g., selling or trading accounts, a user rebranding their own account, etc.) or unwillingly (e.g., compromised account). The vast majority of prior work describe specific instances of account repurposing as a result of compromised accounts or purchased accounts.

As of December 2022, Elmas et. al is in the publication process to describe repurposed accounts on Twitter [2]. In their work they define misleading repurposing as altering account name and other attributes to use for a new purpose while maintaining all followers. They conduct a large-scale study of repurposed Twitter accounts, and develop a classifier

to flag potentially repurposed accounts. We build on their findings but differentiate our work by presenting several case studies of accounts that exhibit malicious behavior. We argue that repurposing accounts is not only misleading but malicious and should explicitly violate Twitter policy. We use this to propose improvements to Twitter Policy.

# 3 Methodology

## 3.1 Definitions

We define and characterize the repurposing of accounts as follows:

**A repurposed account involves a drastic change in content but not necessarily the person operating the account. There are many reasons why an account is repurposed including, but not limited to, a compromised Twitter account, an account transfer, or a rebranded account run by the same user.**

A user repurposes an existing account in order to take advantage of the gained influence of the account for a new purpose including political motivations, self-promotion, or monetary gain. Potential steps that a user might take to repurpose an account involve changing the username significantly, deleting previous Tweets, and changing the biographical data. To the person repurposing the account, it is advantageous to change all of these aspects as expediently as possible so that users cannot detect the account changes and make the decision to unsubscribe from the account.

We define a **benign** repurposed account to be a repurposed account without motivations of misleading their follower base. For example, a fan account for one singer changing into a fan account for another singer. We define a **malicious** repurposed account to be a repurposed account with motivations involving self-promotion, monetary gain, phishing, malware, or including sexually explicit content.

To describe how repurposed accounts evade current Twitter policy we summarize relevant portions of the policy that prohibits the following:

- **Misleading or deceptive identities** defined as posing as an existing entity in a confusing or deceptive manner [12].
- **Inauthentic engagements** defined as an attempt to make accounts or content appear more popular or active than they are. Activity like purchasing followers is in violation of this term [12].
- **Account transfers or sales** defined as "selling, purchasing, trading, or offering the sale, or trade of Twitter accounts, usernames, or temporary access to Twitter accounts" [12].
- Twitter's Ban Evasion Policy states that a user "can't circumvent a Twitter suspension, enforcement action, or anti-spam challenge. This includes any behavior intended to evade any Twitter remediation, such as creating a new account or repurposing an already-existing account." This is only applicable in the case of ban evasion. [10].

Account repurposing does not fall under misleading or deceptive identities because the repurposed account can be run by a legitimate user that simply uses the existing account to have an established follower count. Inauthentic engagement and account transfers or sales only specifies buying and selling of accounts, followers, and likes. Additionally, Twitter's policy mentions repurposing in the context of prohibiting banned users from evading a ban.

## 3.2 Assumptions

As stated earlier, we assume that repurposed accounts attempt to erase identifying attributes of the previous account use by significantly changing noticeable attributes. Therefore, the following assumptions can be made.

- **A large number of significant username changes:** Many username changes are seemingly legitimate. For example, small changes in the letter ordering or a single phrase carried through (e.g., borahae-clouds, borahae-cloud, and borahae_borahe). These are indicative that a user is not aiming to completely repurpose the account. Significant username changes are categorized to be drastically distinct usernames not carrying over elements from previous usernames.
- **Many username changes:** We recognize that legitimate users may still drastically change their username. As a result, we conclude that users with more than 3 significant username changes over a 2-year span aim to repurpose their account.
- **High follower counts:** As noted by Elmas et. al, repurposed accounts typically have higher follower accounts. We also hypothesize that a desirable account to repurpose would have a large number of followers because the greatest appeal of a repurposed account is an existing influence. Malicious actors could simply create a new account if they are not motivated by follower count. More specifically, we set a 5000 follower threshold to measure large influence which we establish based on the precedent set by Twitter in determining if a profile is included in their own data set.
- **Large number of deleted Tweets:** We assume that users will attempt to conceal the previous usage of the account by deleting Tweets. The threshold we set is 1000 or more deleted Tweets as we concluded that manually deleting 1000 Tweets requires significant effort.

- **Sufficiently long account lifetime:** We assume that the repurposed account lifetime must be active across a two-year span. We justify this assumption with the claim that it is difficult to track significant changes in the accounts without having enough information about the account's Twitter usage before and after the repurposing occurred. Additionally, we assume that an account would need time to build a following and has gone undetected by Twitter, meaning it likely did not exhibit bot-like behavior or violate Twitter guidelines (e.g., buy followers, distribute spam). These behaviors are well studied be previous and related work.

### 3.3 Dataset

The data set we used consisted of a 1% sample stream of real-time Tweets annotated with Perspective scores using the Perspective API, a tool that uses machine learning models to label and score negative, or toxic, content [7]. Each row in our data set contains the tweet, its metadata, and the user information.

The data contains Tweets from July 10, 2020 to December 12, 2020 and May 13, 2022 to present day (December 2022). We used the data from August to October in 2020 and 2022 to limit the amount of data that needs to be processed while maintaining more recent information. There is data missing from September 5, 2020 to September 8, 2020 and from October 29, 2022 to October 31, 2022. There is also data missing from several hours during two days in 2020 and from five days in 2022 due to machine hardware issues.

### 3.4 Identification Methodology

We use the assumptions listed in Section 3.2 to further refine our data set and identify accounts that have been verifiably repurposed. We are able to identify the account with which a profile is associated through the *User ID* value stored alongside each tweet in the data set. This *User ID* value will not change throughout the lifetime of the account. Table 1 shows the data filtering steps taken along with the number of users identified at each step. These steps are described in further detail below.

1. Across our sampled data set, we find 29,351,800 distinct *User IDs*, or accounts.

2. 1,604,509 of these accounts were found to have changed their username at least once.

3. We find that of the users that changed their usernames, 611,070 of them exist across 2020 and 2022. A user may not persist across the entirety of the data set due to one of the following reasons: the user was deleted before any 2022 Tweets were collected, the user was created after the 2020 data was collected, or the user simply did not appear in one of the data collection periods. 63% (178,404/282,288) of users that appeared in 2022 but not 2020 are new accounts. The fraction of accounts found only in 2020 data due to account deletions is yet to be determined. Nevertheless, we intend to focus on the user accounts that persist across both 2020 and 2022 because they either resemble legitimate accounts or inauthentic accounts that have bypassed Twitter's account removal system seeing that they have yet to be suspended from Twitter after existing for at least two years.

4. To further narrow down our dataset, we filter the *User IDs* that have at least three significant username changes, finding 109,222 accounts. In order to pare all of the Tweets down and identify significant username changes, we grouped all of the Tweets by *User ID*, and then found the list of unique usernames attached that *User ID*. At this point, there is still a chance that the *User IDs* are a minor, legitimate change and not related to the repurposing of accounts. We used the Levenshtein distance, or a measure of similarity between two strings which provides the number of deletions, insertions, or substitutions required to turn one string into another. Between each pair of unique usernames, we calculated the Levenshtein distance normalized by the length of the strings. The final list of unique usernames only included usernames where this normalized distance was significant enough. If the *User ID* had more than three significantly different usernames, we continued considering it for further filtering.

5. Of these accounts, we find that as of November 31, 2022 only 45,635 still exist on the platform.

6. Of these users, we follow the Twitter precedent of only considering accounts with more than 5000 followers at some point between 2020 and 2022. This pared the data set even further down to 3,668 users.

7. Lastly, following our assumption of repurposed accounts having made significant effort to remove the previous account presence, we exclude accounts who have not deleted at least 1000 Tweets. This results in just 104 users which we manually verified.

### 3.5 Limitations

We recognize that our approach has significant limitations and address them in the following.

- There were most likely many repurposed accounts that this methodology filtered out. However, we choose to liberally filter our data in order to result in a manageable data set of repurposed accounts to manually verify.

- Some of our thresholds are subject to opinion and arbitrary. For example, the threshold of greater than 3 user

Table 1: Steps taken to identify any repurposed accounts and the number of users identified at each stage that satisfy all the criteria before it.

| Filtering Operation | Number of Users Left |
|---|---|
| (1) No filtering applied | 29,351,800 |
| (2) More than 1 username change | 1,604,509 |
| (3) Account persists across the entire dataset | 611,070 |
| (4) At least 3 significant username changes | 109,222 |
| (5) Still exist in December of 2022 | 45,635 |
| (6) More than 5000 followers | 3,668 |
| (7) Deleted more than 1000 Tweets | 104 |

Table 2: Types of account changes observed and their classification.

| Type of Account Change | Classified As A Repurposed Account |
|---|---|
| Legitimate name changes | No |
| Slight content variations on a common theme | No |
| Switching between one topic account and another topic | Yes (Benign) |
| Switching between a personal and a business account | Yes (Malicious) |
| Switching from a personal account to another personal account | Yes (Malicious) |

name changes or the 1000 Tweet deletion threshold were both arbitrary. These thresholds, however, allowed us to filter the data set down significantly and increase the likelihood that we find repurposed accounts. With more time, these thresholds can be tested and refined to be more precise.

- We only have an external view of changes across *User IDs*. Those with a much richer data set, including access to all username changes, will have a better view into user behavior.

- This methodology can only prove the existence of malicious repurposed accounts and not the prevalence, meaning that our results are the lower bound for all repurposed accounts on Twitter. This suggests that malicious account repurposing could be much more prevalent.

## 3.6 Verification

The ground truth of whether an account is run by two different individuals is difficult to verify. One individual can drastically change their Twitter account for another purpose. However, account repurposing is more easily identified via manual inspection of longitudinal data. However, since the data set we are using is Tweets from two periods of time two years apart, there is a chance that a user may have more gradually changed their content. In this paper, we present case studies of repurposed accounts that we are confident were repurposed.

To verify if an account was repurposed, we conduct two scans of manual inspection.

1. Accounts with the most username changes

2. Accounts existing in both 2020 and 2022

Our first manual inspection led us to believe that many of the less obvious username changes, username changes to very different strings, or even usernames with randomly generated strings no longer exist on Twitter. In our second manual inspection, we found the maximum number of username changes to be 53 as opposed to the maximum of 86 username changes across all accounts. We note that of the twenty accounts analyzed that several are benign or hard to categorize (typically fan accounts), two were private, and two were deleted. Most still exhibit suspicious behavior, including explicit material, thousand of Tweets that only exist within the past few weeks, spamming of the same Tweets, giveaway promotions, or more.

## 3.7 Ethical Considerations of Methodology

Since our data set involves longitudinal data and borders the underground market of account sales, there are ethical considerations to storing and operating with this Tweet data. All of the data is stored on secure machines in the Stanford University network.

Storing this longitudinal data has privacy concerns as users may not be explicitly aware that this data is being collected and stored. However, we consider the benefit of tracking the

Tweet data over time. There is greater benefit from understanding the malicious repurposing of Twitter accounts. Changes in ownership or sudden changes in Tweet content especially political information, links, promotion, and sensitive data is misleading and harmful to users. Therefore, by studying repurposing behavior and collecting this data, we are able to provide proposals to Twitter to mitigate harm to users. Additionally, we do not publish or share individual data or case studies that could present as defamation or harmful to any individuals.

## 4 Results

We observe the types of account changes shown in Table 2. An example of each type of account change is detailed below.

- **Legitimate name changes:** *Jane Smith Doe* $\longleftrightarrow$ *Janey*.
- **Slight content variations on a common theme:** inspirational quotes $\longleftrightarrow$ meditation quotes
- **Switching between one topic account and another topic:** cooking content $\longleftrightarrow$ dog content
- **Switching between a personal and a business account:** personal account $\longleftrightarrow$ e-sports team
- **Switching from a personal account to another personal account:** *Jane Smith Doe* $\longleftrightarrow$ *Joe Citizen*

We do not classify the legitimate name changes and slight content variations as repurposed accounts. This is because there is a higher likelihood that these accounts were not in fact repurposed due to high similarities. We classify topic, person, and account type switching as account repurposing. However, we do not classify topic switching as malicious and acknowledge a limitation of our classification structure here. Without further analysis, it cannot be said that topic switching is not simply the switching interests of an individual. One case where we found the most *gray area* was fan account who switched content between several Korean pop music singers or actors. Therefore, we classify this entire category as benign account repurposing. Switching between personal and business accounts or changing from one person to a significantly different person is classified as malicious as there is a clear attempt to mislead the following base and Twitter user space at large.

From our manual inspection, we offer additional recommendations for filtering out false positive results, the first being identifying common substrings across multiple profile attributes. We notice that identifying overlapping or similar profile information such as the username, screen name, and biographical information can help determine if the account is not repurposed. For example, a user might significantly change their username and remove their biographical information completely but add information such as age and location to their screen name instead that is consistent. We argue that while it is useful to understand the differences across a single attribute like screen name, future work should also take holistic profile information into consideration. Second, we want to highlight the importance of identifying the account type based not just on profile attributes but Tweet content. An example of this is a fan account for a group or organization. The account changed their profile identity from one member of the group to a different member, while still keeping the purpose and content of the account the same.

We also identify characteristics of true repurposed accounts. We find accounts that are repurposed many times. Repurposed accounts do not necessarily wipe out every previous tweet. The individual repurposing the account may only delete tweets that can be easily linked to previous account identities. Additionally, we find that some of these repurposed accounts have anomalous engagement. For example, one of the accounts we investigate has tens of thousands of likes for a week of tweets, but only a couple of likes for every other tweet.

## 5 Case Studies

We present three case studies that classify as malicious repurposing of a Twitter account.

### 5.1 Case Study 1


Figure 2: Current Twitter profile of Case Study 1.

In this first case, we see a repurposed account involving the switch between two personal accounts that are sufficiently different. Table 3 shows the account information for an account with the same *User ID* at two different points in time. This account goes from a politically-left leaning individual with

significantly less followers and 1,245 Tweets to an account who is politically-right leaning with many more followers and only 35 Tweets. This shows a significant decrease in Tweets, indicating many were deleted, with a jump in followers. Figure 2 shows the current profile of this case study.

Table 3: Case study 1 username, biographical information, follower count, and number of Tweets.

| **@disillusioned05** | **@humphrers** |
|---|---|
| Feminist. Trans. LGBTQ+. Remainer. Cat lover. Socialist. Vegan. European. Pacifist. Leftie. Do-gooder. Anti-racist. BlackLives-Matter EndChildFood-Poverty FBPE | Proud englishman. Centre-right. Lefty scroungers & remainers = [vomiting emoticon] Retired. Priti Patel fan. The woke youth of today wouldn't last in a war. Anti student. [UK flag emoticon] |
| 973 followers | 6,794 followers |
| 1,245 Tweets | 35 Tweets |

We can assume that the previous follower base before repurposing was politically-left leaning. By repurposing the account to a politically-right leaning account, there is potential harm to the users as one could speculate an attempt to push a political ideology. As a result, we conclude this type of repurposing to be malicious.

## 5.2 Case Study 2

In the second case study, we see an account that has switched from posting sexually explicit content (personal account) to an essay writing service (business account). This example falls into the category of a personal account that has been converted to a business account and is therefore classified as malicious account repurposing. Table 4 shows the account information for an account with the same *User ID* at two different points in time. Similar to the last case study, this account has a rise in follower with a drop in Tweets, indicating many Tweets were deleted and there was an attempt at repurposing this account. Figure 3 shows the current profile of this case study.

The follower base for the previously sexually explicit account most likely does not much overlap with people who are looking for an essay writing service. Additionally, this type of account repurposing is hoping to mislead the previous follower base for monetary gain as this is now a business. As a result, we also can conclude this type of repurposing to be malicious.


Figure 3: Current Twitter profile of Case Study 2.

Table 4: Case study 2 username, biographical information, follower count, and number of Tweets.

| **@boneLessKe** | **@lurlyscholars** |
|---|---|
| I am BoneLess, Happy Polygamous Man, Team Red Devils | Essays ‖ Research papers ‖ Maths ‖ Psychology ‖ Accounting ‖ Physics ‖ Statistics ‖ Online classes and much more. Email: globalessaywriters23@gmail.com |
| 10,024 followers | 21,267 followers |
| 22,024 Tweets | 11,147 Tweets |

### 5.3 Case Study 3

In the last case study, we see a another repurposed account from a personal to a business account offering professional services. Table 5 shows the account information for an account with the same *User ID* at two different points in time. This account was previously an activism account for human rights and was repurposed to an account focusing on entrepreneurship, fashion and giveaways. Again, we see a decrease in Tweets and an increase in followers suggesting an attempt to repurpose the account. Figure 4 shows the current profile of this case study.

Table 5: Case study 3 username, biographical information, follower count, and number of Tweets.

| **@sir_CharlesOgu** | **@Fashion_Hub4** |
|---|---|
| Human right Activist. [eye emoticon]. Leader Civil Rights Movement | interest in fashion • Fashion designer • Free online courses for people having interest in fashion • L!NK COMING SOON |
| 4,394 followers | 25.9K followers |
| 3,081 Tweets | 2,479 Tweets |


Figure 4: Current Twitter profile of Case Study 3.

This is another attempt to mislead a follower base and Twitter at large that a business has more influence for the purpose of monetary gain. This, again, presents harm to users and we can conclude that this type of repurposing is malicious.

## 6 Twitter Policy Recommendation

We conclude that many cases of Twitter account repurposing are malicious. Therefore, we recommend that Twitter refine their Terms of Service to include robust definitions for terms like *inauthentic behavior* and *malicious behavior* that encompass these cases of account repurposing outside of ban evasion policy. We also suggest Twitter include clauses excluding legitimate user changes such as transitioning or "coming out" in the LGBTQIA+ community.

Without longitudinal data, it is close to impossible for the average user to detect that they are following a repurposed account just by glancing at the Twitter profile. We recommend Twitter implement several features to mitigate these risks:

- Limit the number of username changes within a given period of time and require username reviews if the account reaches a large portion of users. More work will need to be done to identify the recommended amount of time between permitted username changes. This technique is used by other popular social media platforms such as Instagram [5].
- Add a simple way for users to report account repurposing through the Twitter interface. In this paper, we use longitudinal data to identify whether or not a Twitter account has been repurposed. This was possible due to the scale of our data set. This task is herculean across all of Twitter, without considering the ethically dubious nature of storing all Tweets after deletion for all of Twitter. Therefore, the simplest way to identify if an account has been repurposed is by allowing the follower base to report it. To account for the fact that it is undetectable if an account has been repurposed, we recommend Twitter display the previous username for a brief period of time next to the current username. This period of time would need to be refined and we leave this to Twitter to decide as they have the most in depth knowledge on this subject.

## 7 Conclusion

Using longitudinal data, identifying repurposed accounts is possible and simpler than trying to identify when accounts are transferred. The vocabulary used in Twitter's usage policy needs to be robustly defined and prevent malicious account repurposing explicitly. We acknowledge the gray area introduced with fan accounts (benign repurposed accounts) and propose that further research be done in this area. We aim for this paper to spurn further research in this field to make social media safer for users overall.

## 8 Acknowledgments

We would like to thank Catherine Han and the Empirical Security Research Group at Stanford University for providing

us with the data set used in this paper. We would additionally like to thank Deepak Kumar for his help in obtaining the data set.

## References

[1] Andrew Chu, Arjun Arunasalam, Muslum Ozgur Ozmen, and Z Berkay Celik. Behind the tube: Exploitative monetization of content on youtube. In *31st USENIX Security Symposium (USENIX Security 22). Boston, MA: USENIX Association. URL https://www. usenix. org/conference/usenixsecurity22/presentation/chu*, 2022.

[2] Tuğrulcan Elmas, Rebekah Overdorf, Ömer Faruk Akgül, and Karl Aberer. Misleading repurposing on twitter. *arXiv preprint arXiv:2010.10600*, 2020.

[3] Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, and Ben Y Zhao. Detecting and characterizing social spam campaigns. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, pages 35–47, 2010.

[4] Chris Grier, Kurt Thomas, Vern Paxson, and Michael Zhang. @spam: the underground on 140 characters or less. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 27–37, 2010.

[5] Instagram. When you can change your instagram username to a name you've used before. https://help.instagram.com/876876079327341. Accessed on 2022-12-16.

[6] Myra Nizami. How to make money on twitter. https://smallbiztrends.com/2021/12/how-to-make-money-on-twitter.html. Accessed on 2022-12-16.

[7] Perspective. Perspective api. https://perspectiveapi.com/. Accessed on 2022-11-11.

[8] Gianluca Stringhini, Manuel Egele, Christopher Kruegel, and Giovanni Vigna. Poultry markets: on the underground economy of twitter followers. *ACM SIGCOMM Computer Communication Review*, 42(4):527–532, 2012.

[9] Kurt Thomas, Damon McCoy, Chris Grier, Alek Kolcz, and Vern Paxson. Trafficking fraudulent accounts: The role of the underground market in twitter spam and abuse. In *22st USENIX Security Symposium (USENIX Security 22). Washington, D.C.: USENIX Association. URL https://www. usenix.org/system/files/conference/usenixsecurity13/sec13-paper$_i$homas.pdf*, 2013.

[10] Twitter. Ban evasion policy. https://help.twitter.com/en/rules-and-policies/ban-evasion. Accessed on 2022-12-16.

[11] Twitter. Media studio monetization. https://help.twitter.com/en/using-twitter/how-to-monetize-in-media-studio. Accessed on 2022-12-16.

[12] Twitter. Misleading and deceptive identities policy. https://help.twitter.com/en/rules-and-policies/twitter-impersonation-and-deceptive-identities-policy. Accessed on 2022-12-16.

[13] Eva Zangerle and Günther Specht. " sorry, i was hacked" a classification of compromised twitter accounts. In *Proceedings of the 29th annual acm symposium on applied computing*, pages 587–593, 2014.