Chad Ballay

CYB410-342N

9/13/2020

Week 1 – Twitter Account Security

**Twitter is a mainstay of people of all ages to keep in touch with each other and seemingly validate their own existence. What measures are in place to secure Twitter accounts and could be improved in securing them?**

Twitter has become a public communication channel while remaining a non-governmental entity. This leaves it in a precarious role of being a public utility while under private control. With this in mind there are certain layers of defense that have been taken to protect user accounts and information.

# User Training

Best practices are communicated in a clear manner from Twitter’s website. The documentation explains concepts like strong passwords, never share your credentials, recommends login verification, and other basic user security best practices.

<https://help.twitter.com/en/safety-and-security/account-security-tips>

# Account Alerts

Proactively, Twitter will send a notification when any of several key account details are changed. Often this is an attacker’s first step after gaining access to a user’s account. For example, when a user’s email address associated with their account is updated, a notification will be sent to the previously used account informing of this change in data. If a new device signs into the user’s Twitter account a notification is sent. All of these help ensure that suspicious behaviors are caught early on.

<https://help.twitter.com/en/managing-your-account#notifications>

# User Verification

For most users, a web of trust or just blind acceptance is enough verification that the account is communications from who they say they are. Through a human dependent process of verification, certain users that have been deemed noteworthy can undergo a verification process. This process has changed multiple times, but the gist is that through secondary and tertiary means the user is able to prove who they are and then tie this authentication to the Twitter account they use. These verified accounts are represented with a blue checkmark. While this process does not scale well it has meant that when I see a tweet from an account that has been verified that I can strongly assume that those are the actual words of the purported account holder.

<https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts>

# Spam, Impersonation, Troll Accounts

No system is perfect and fake accounts do occur with some frequency. An additional control mechanism is the reporting feature that any users can start. If an account is breaking the TOS or otherwise inappropriate, individual users can submit a request for the account to be reviewed. Individually one users report may not be actionable but collectively this helps focus the review process to quickly remove bad actors from the Twitter system.

<https://help.twitter.com/en/safety-and-security#spam-and-fake-accounts>

# Tentative Next Steps

I personally do not agree the expansion of verified accounts will ever be a completed task. Rumors of using the REAL ID system to tie Twitter account to a person become a very complex issue due to Twitter’s unique status as a private company being used for public works. The first amendment entanglements are numerous and troubling if rushed decisions set precedent. After the security breach of summer 2020, it is apparent that something is needed. What that something is unclear to me though. More monitoring of trends and behavior changes at the aggregate level on accounts rather than individual account monitoring seems to be one battle front. If multiple verified accounts share the exact same message a review and response may be needed by Twitter.

<https://www.cnn.com/2020/07/26/tech/twitter-hack-remote-working-security-risks/index.html>