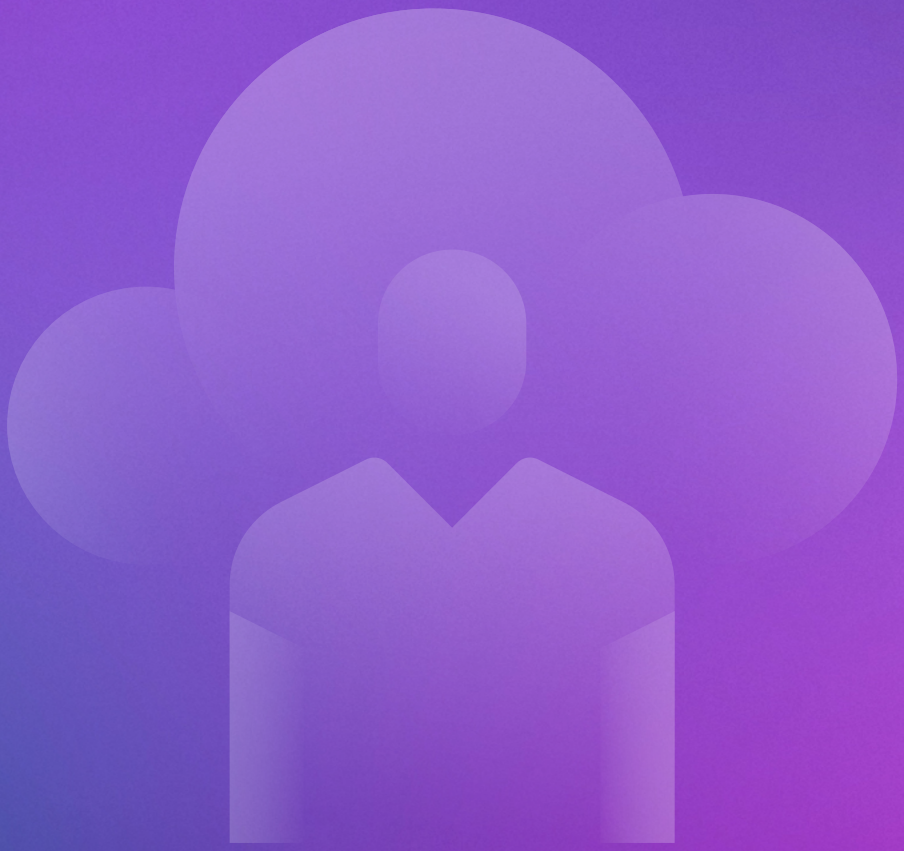
HUMAN

FAKE ACCOUNTS ARE NOT YOUR FRIENDS!

INFLATED USER BASES AND FAKE ENGAGEMENT CAUSE MORE HARM THAN GOOD, ESPECIALLY WHEN THE ARTIFICIAL ACCOUNTS ARE BASED ON STOLEN HUMAN IDENTITIES.



Written by Jonathan Care,
Contributing Writer, Dark Reading

INTRODUCTION

Growth in the number of new accounts looks great, but if fake accounts get in that mix, they are not providing the value you (and your investors) need. If you are a social media platform striving for growth, fake accounts may seem like the answer to your prayers — something you can show investors to demonstrate your reach. And to the end user, all those accounts that listen to music online or follow us on social media seem great. But the reality is that fake accounts are harmful, even before the truth comes to light.

It's especially damaging when bots use real human data, stolen and sold on the Dark Web, to create these fake accounts. And when they are exposed to sunlight, as the situation with Elon Musk's stalled acquisition of Twitter has shown, the effects can be unexpected and rampant, quickly taking on a life of their own.

We're going to look at what fake accounts mean, why they exist, and what you can do to combat this pernicious adversary.

"Cybercriminals have proliferated sophisticated bots and spam accounts across social media platforms with limited accountability, and the combined result is diminished trust in the brand, a negative user experience, and a negative impact on the company's valuation and bottom line."

— Tamer Hassan, co-founder and CEO of Human Security

ENTER THE BILLIONAIRE

Love him or hate him, you cannot deny the impact Musk has made on the tech industry. But second-guessing his motives and actions is very much like my dog trying to work out the significance of my sitting at my desk drumming my fingers on the keyboard all day.

When I spoke with Tamer Hassan, co-founder and CEO of Human Security, I asked him what he believes is the core challenge facing any investor looking at Twitter.

"It's really all about the question, 'What would you do if you could look like a million humans?' The answer is a lot," he said. "Cybercriminals have proliferated sophisticated bots and spam accounts across social media platforms with limited accountability, and the combined result is diminished trust in the brand, a negative user experience, and a negative impact on the company's valuation and bottom line."

TWITTER & THE TRAGEDY OF THE DIGITAL COMMONS

Twitter is an increasingly rare Internet resource. It is a common platform connecting humans all over the world and, with some rare exceptions, does not inhibit or censor free expression. As with most common goods, it is subject to overuse; the phrase "tragedy of the commons" originated to describe people overusing grassy common land to graze their livestock. As anyone who has dipped a toe into the Twitter stream knows, the slew of tweets is overwhelming and impossible to keep up with. This is made worse because, along with all of the humans desperate to air their opinions, points of view, and excitable investment plans, there are The Bots.

Bots are part of much of our life nowadays. Those of us using Office365 are familiar with the coy daily email saying, "Hey, we aren't analyzing what you do or the content of your inbox, but here's some stuff to be aware of," and of course, on Twitter there are beneficial bots and harmful bots. Many bots watch for tweets that seem to relate to a particular subject (for example, #cybersecurity), and then amplify those tweets to their audiences. And of course, many will try and game these amplifiers, sometimes using bots of their own. And so the overgrazing continues.

NO ONE SHOULD PAY FOR FALSE VOLUME, EVEN BILLIONAIRES

The primary incoming revenue stream for social platforms is advertising, which is driven by how many interested eyes can be shown targeted ads that are likely to lead to conversion. It therefore follows that the value of any social platform lies in the number of active users, whether it be a general-purpose networking platform such as Twitter, a narrow-purpose use case such as music, or even accommodation rentals (inactive users are just sludge at the bottom of the well). Bots, while they may generate activity, defraud advertisers by artificially inflating the user count.

Musk is understandably squeamish about paying for accounts that have zero (or even negative) lifetime value. When I asked about what a company can do about bots, Hassan commented, "Having the right protections in place, including transparency and regulation around the use of automation, to ensure they have a genuine view of human users on their platform can help brands establish greater credibility while also stopping cybercriminals from impacting their business."

Musk very publicly tried to withdraw from the Twitter acquisition, which has generated continuing legal ramifications. If we take his statements at face value, then the clear message is that bots and other fake accounts are bad business. Considering the ways that future Twitter (or any social media platform) could make money, being a trustworthy source of curated identity that doctors, banks, governments, and any other interested party (including peer-to-peer) can rely on would be a significant advantage.

HERE'S MUDGE IN YOUR EYE

One of Musk's stated concerns about the Twitter acquisition is that he has no certainty about how many of the platform's 396.5 million accounts are human. To add fuel to Twitter's bonfire of the vanities, its former CISO, Peiter "Mudge" Zatko, has blown the whistle on poor operational security controls, nonexistent software governance, and (you guessed it) inadequate user enrollment verification. In other words, no one knows how many users are bots, and what vulnerabilities exist in the platform that can be exploited by unfriendly groups — some of which are backed by nation-states.

As a former Facebook security engineer pointed out to me, "Mudge has a decades-long reputation of being highly ethical and one of the most respected practitioners in the cybersecurity community." When I asked whether they believed Mudge's claims about foreign intelligence infiltration, the response was, "I believe enough of it not to care about the rest."

Robert Graham takes a different view in his Cybersect blog, which contrasts the focus of a cybersecurity activist with that of a corporate executive. An executive's primary objective is to further the interest of the company and its shareholders, he wrote, which does not correlate with the ideals of many cybersecurity activists. In his view, Mudge has allowed his passion for cybersecurity excellence to overwhelm his responsibilities as an executive.

IDENTITY AS A COMMODITY

Identity is the cornerstone of cybersecurity. When an identity is successfully compromised, all of the other security controls will fold up and get out of the attacker's way. The opportunity for Twitter to provide an identity service based on its user base is a significant one.

It is clear, however, that if we cannot trust that the identities being asserted and corroborated by Twitter are genuine, then Twitter's usefulness in this area will always be limited. Twitter asserts that the cost of validating every account (and giving us all a little blue tick) is prohibitive, however, as the lifetime value of each Twitter account is very low.

I'm sure that Twitter is well aware of its security gaps. Indeed, a good use for some of Musk's proposed investment, if the company can still get it, would be to clean up the town square and correct the tragedy of the digital commons that we discussed earlier.

This is why identity is important, in particular being able to prove that a specific account is being operated by a human. If we manage to turn Twitter into a place where free speech is valued precisely because the speakers are identified as human, then its value — to investors, the Twitter team, and most importantly, its users — will skyrocket.

https://www.darkreading.com/edge-articles/fake-accounts-are-not-your-friends-

About HUMAN

HUMAN is a cybersecurity company that safeguards 1,200+ brands from digital attacks including bots, fraud and account abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN. **To Know Who's Real, visit www.humansecurity.com.**