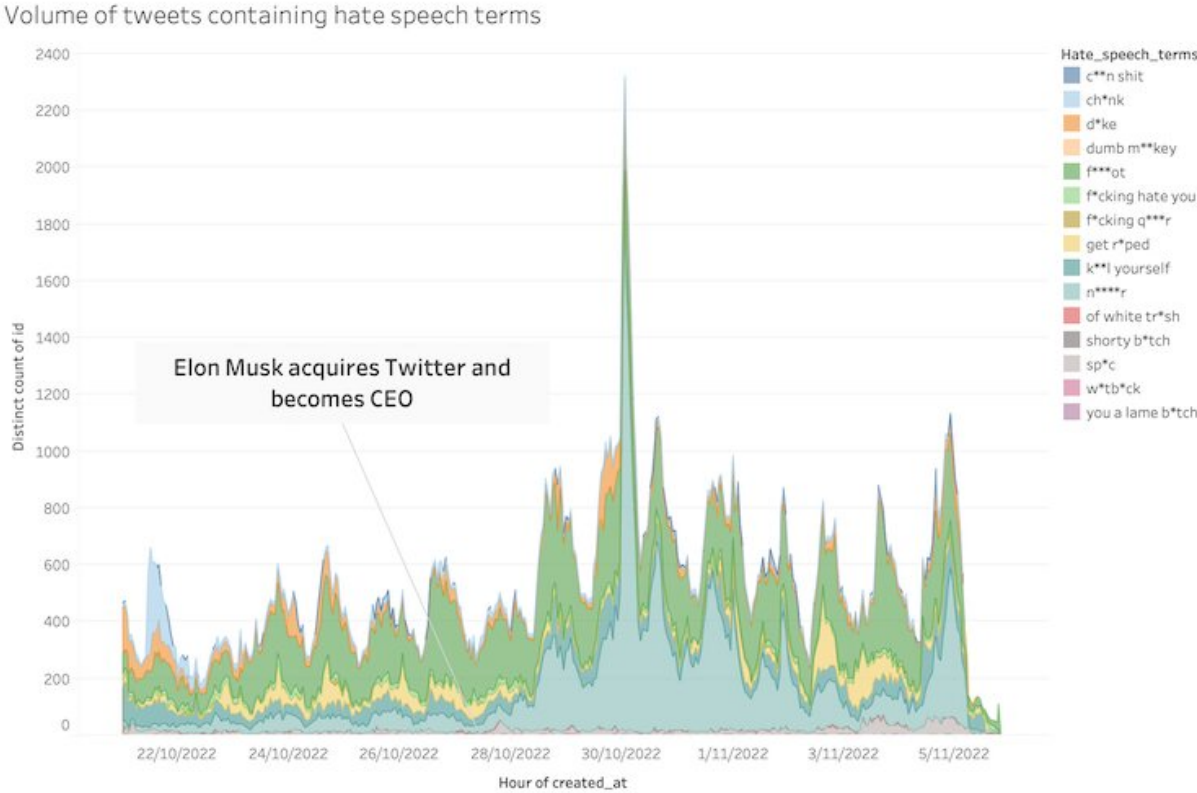# Thinking of breaking up with Twitter? Here's the right way to do it

November 22 2022, by Daniel Angus and Timothy Graham

Volume of tweets containing hate speech terms.

After a few chaotic weeks it's clear Elon Musk is intent on taking Twitter in a direction that's at odds with the prevailing cultures of the diverse users who call it home.

Musk has now begun [reinstating](#) high-profile users—including Donald Trump, Alex Jones and Kanye West—who had been removed for repeated violations of community standards.

This comes off the back of a mass exodus of Twitter staff, including thousands that Musk [unceremoniously fired](#) via email. The latest wave of resignations came after an ultimatum from Musk: employees would have to face "extremely hardcore" working conditions (to fix the mess Musk created).

All of this points to a very different experience for users, who are now decamping the platform and heading to alternatives like Mastodon.

So what threats are we likely to see now? And how does one go about leaving Twitter safely?

#TwitterShutDown

With [so many experienced](#) staff leaving, users face the very real possibility that Twitter will experience significant and widespread outages in the coming weeks.

Enterprise [software experts](#) and [Twitter insiders](#) have already been raising alarms that with the World Cup under way, the subsequent increase in traffic—and any rise in opportunistic malicious behavior—may be enough for Twitter to grind to a halt.

Aside from the site going dark, there are also risks [user data](#) could be breached in a cyberattack while the usual defenses are down. Twitter was exposed in a massive cyberattack in August this year. A hacker was [able to extract](#) the [personal details](#), including phone numbers and email addresses, of 5.4 million users.

One would be forgiven for thinking that such scenarios are impossible. However, common lore in the technology community is that the internet is held together by chewing gum and duct tape.

The apps, platforms and systems we interact with every day, particularly those with audiences in the millions or billions, may give the impression of being highly sophisticated. But the truth is we're often riding on the edge of chaos.

Building and maintaining large-scale social software is like building a boat, on the open water, while being attacked by sharks. Keeping such software systems afloat requires designing teams that can work together to bail enough water out, while others reinforce the hull, and some look out for incoming threats.

To stretch the boat metaphor, Musk has just fired the software developers who knew where the nails and hammers are kept, the team tasked with deploying the shark bait, and the lookouts on the masts.

Can his already stretched and imperiled workforce plug the holes fast enough to keep the ship from sinking?

We're likely to find out in the coming weeks. If Twitter does manage to stay afloat, the credit more than likely goes to many of the now ex-staff for building a robust system that a skeleton crew can maintain.

Hate speech and misinformation are back

Despite Twitter's claims that hate speech is being "mitigated", our analysis suggests it's on the rise. And we're not the only researchers observing an uptick in hate speech.

The graph below shows the number of tweets per hour containing hate

speech terms over a two-week period. Using a [peer-reviewed hate speech lexicon](#), we tracked the volume of 15 hateful terms and observed a clear increase after Musk's acquisition.

Misinformation is also on the rise. Following Musk's swift changes to blue tick verification, the site tumbled into chaos with a [surge of parody accounts](#) and misleading tweets. In response, he issued yet another stream-of-consciousness policy edict to remedy the previous ones.

With reports that the entire Asia-Pacific region has only one working [content moderator left](#), false and misleading content will likely proliferate on Twitter—especially in [non-English-speaking countries](#), which are especially at risk of the harmful effects of unchecked mis- and disinformation.

If this all sounds like a recipe for disaster, and you want out, what should you do?

Pack your bags

First, you may want to download an archive of your Twitter activity. This can be done by clicking through to Settings > Settings and Support > Settings and Privacy > Your Account > Download an archive of your data.

It can take several days for Twitter to compile and send you this archive. And it can be up to several gigabytes, depending on your level of activity.

Lock the door

While waiting for your archive, you can begin to protect your [account](#). If

your account was public, now might be a good time to switch it to protected.

In protected mode your tweets will no longer be searchable off the platform. Only your existing followers will see them on the platform.

If you're planning to replace Twitter with another platform, you may wish to signal this in your bio by including a notice and your new username. But before you do this, consider whether you might have problematic followers who will try to follow you across.

Check out

Once you have downloaded your Twitter archive, you can choose to selectively delete any tweets from the platform as you wish. One of our colleagues, Philip Mai, has developed a [free tool](#) to help with this step.

It's also important to consider any direct messages (DMs) you have on the platform. These are more cumbersome and problematic to remove, but also likely to be more sensitive.

You will have to remove each DM conversation individually, by clicking to the right of the conversation thread and selecting Delete conversation. Note that this only deletes it from your side. Every other member of a DM thread can still see your historic activity.

Park your account

For many users it's advisable to "park" their account, rather than completely deactivate it. Parking means you clean out most of your data, maintain your username, and will have to log in every few months to keep it alive on the platform. This will prevent other (perhaps malicious)

users from taking your deactivated username and impersonating you.

Parking means Twitter will retain some details, including potentially sensitive data such as your phone number and other bio information you've stored. It also means a return to the platform isn't out of the question, should circumstances improve.

If you do decide to deactivate, know that this doesn't mean all your details are necessarily wiped from Twitter's servers. In its [terms of service](#), Twitter notes it may retain some user information after account deactivation. Also, once your account is gone, your old username is up for grabs.

Reinforce the locks

If you haven't already, now is the time to engage two-factor authentication on your Twitter account. You can do this by clicking Settings > Security and account access > Security > Two-factor authentication. This will help protect your account from being hacked.

Additional password protection (found in the same menu above) is also a good idea, as is changing your password to something that is different to any other password you use online.

Once that's done, all that's left is to sit back and pour one out for the bird site.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation