THREE THINGS: THE EARLY BIRD GOT WORMED

[*NB: Check the byline, thanks. /~Rayne*]

The self-ownage continues at Twitter. I don’t even know where to start because there’s just so much damage in the bird app’s debris field.

Let’s go with the problems closest to deaths.

~ ~ ~

The brilliant billionaire who overpaid for Twitter, who thought his Tesla engineers were qualified to determine staffing levels on software created over 16 years they didn’t write, had another brilliant idea.

He played Jenga with code within the platform because the application was too slow.

(I haven’t heard anyone complain about Twitter’s speed in ages, and when there’ve been complaints they’re usually in tandem with a major event flooding the network and system with user requests and tweets.)

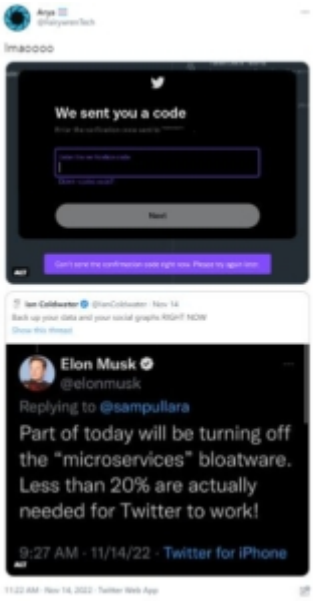
Twitter’s speed hasn’t been a bottleneck to increasing users or profitability.

In the process of unplugging stuff to see if the platform would speed up, a worker who actually knew something about all the legacy code criticized Musk’s absurd efforts.

Free speech absolutist Musk fired him, egged on by his fanboi trolls.

And then users began to experience problems with Two-Factor Authentication (2FA) over Short

Message Service (SMS), otherwise know as text messages.



The security system which allows users to ensure their account can't be accessed by unauthorized persons was broken, preventing users from accessing their accounts.

This also prevented users from checking their accounts to make sure they weren't hacked and their verification worked.

~ ~ ~

Which is why during Sunday's night's mass shooting at University of Virginia, students as well as the public following the story were reportedly confused about UVA's emergency message. They couldn't be sure after Elon Musk's back-and-forth changes to its verification system whether the message they read in Twitter from UVA-Emergency Management was legitimate.

Fortunately students used their own student-developed thread in a mobile app called Yik Yak to validate the emergency. Yik Yak has been problematic in the past, pulled from app stores because of unmoderated toxic behavior, but it was relaunched in 2021 and valuable to students during the shooting lockdown at UVA because Yik Yak limits reach to five miles. In other words, the students knew whoever was using the app was local to campus.

It’s possible the students could have deduced the UVA-Emergency Management tweet was legitimate because it displayed the source of the message — Rave Mobile Safety, an emergency messaging system. Had UVA-Emergency Management’s account been spoofed, a phone or desktop might have appeared instead of Rave.

This detail may not be available for much longer. Musk thinks identifying the source of tweets by device or application is just inconvenient bloatware.

Should we ask UVA students and their parents about Twitter’s bloatware problem?

~ ~ ~

As I noted in my previous Twitter acquisition timeline post, the company has been subject to a Federal Trade Commission consent decree since 2011 because of its failures to assure users' personal data was secure.

From the FTC's 2011 statement:

> …The FTC alleged that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including both access to non-public user information and tweets that consumers had designated as private, and the ability to send out phony tweets from any account.

A $150 million penalty had been levied by the FTC only a month after Twitter and Musk agreed on terms for the acquisition.

And yet Musk noodled around with Twitter Blue and the blue check verification system, affecting the verification status of organizations as well as individuals — none of the changes done with documentation prepared in advance, or with red team testing for quality assurance.

Musk's ham-handed mucking around in microservices temporarily affecting 2FA SMS — some accounts are apparently still affected — was likewise done without advance preparation, and in the face of criticism by seasoned employees who understood the system.

It's worth noting in that same statement by the FTC these last two paragraphs:

> NOTE: A consent agreement is for settlement purposes only and does not constitute an admission by the respondent that the law has been violated. When the Commission issues a consent order on a final basis, it carries the force of law with respect to

> future actions. Each violation of such an order may result in a civil penalty of up to $16,000.
>
> The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. To file a complaint in English or Spanish, visit the FTC's online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357). The FTC enters complaints into Consumer Sentinel, a secure, online database available to more than 1,800 civil and criminal law enforcement agencies in the U.S. and abroad. The FTC's Web site provides free information on a variety of consumer topics. "Like" the FTC on Facebook and "follow" us on Twitter.

Though the FTC might want to rethink that last Follow, persons who felt their personal data was at risk over the last three weeks might want to drop the FTC a note.

~ ~ ~

After reading about the acquisition and the subsequent mass terminations along with the manifold fuck-ups like verification and 2FA SMS, I wonder if Musk and Twitter executives ever notified the FTC of the change in ownership as required by the consent decree.