Threat Briefing:

Social Media Security and Elections

Volume 1

cerby®

Table of contents

Executive Summary

Social media platforms used by popular U.S. political leaders often lack the security controls necessary to prevent disinformation campaigns. U.S. politicians have grown their social presence over the last few presidential elections following a general trend away from mass media, and nation-states have taken notice.

Most of the attention dedicated to security in social media networks focuses on the companies running them. But what about the users, particularly political leaders with huge followings? What can they do to secure their social media accounts?

In this threat briefing, the research team at Cerby set out to evaluate some of the biggest platforms in terms of the security controls they offer their users. Researchers evaluated five prominent social media platforms across critical areas, such as two-factor authentication (2FA), enterprise readiness, and privacy. The research zeroes in on a critical balance: the security and privacy options social media platforms extend to their users and users taking advantage of them.

Using a scale of 0 to 5 for each category (with 5 being the highest possible rating), Facebook took the top prize with an overall score of 3.34. Twitter came in second at 2.75. Taking the third spot was Instagram with 2.68, followed by TikTok at 2.00, and Reddit at 1.95. **Based on the findings, researchers at Cerby are not recommending politicians stop using these platforms but focus their efforts on mature platforms scoring at least 2.6 or higher.** Platforms scoring 2.6 or higher, while currently lacking mature support for enterprise-grade authentication like single sign-on (SSO), offer robust security controls for 2FA with support for emerging standards like Fast Identity Online 2 (FIDO2).

Despite their continued growth as the news medium of choice for voters, the U.S. does not have security standards or oversight for social media platforms. Until this changes, politicians and voters should expect a continued assault from nation-states looking to execute disinformation campaigns.

What is FIDO2?
FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments. It is widely seen as the answer to the problem most users have with password management. FIDO2 is part of a passwordless future.

Background

In 2020, prominent Twitter accounts were hacked. Stars ranging from former President Barack Obama and Michael Bloomberg to Warren Buffett and Kanye West—with a collective audience of 250 million—suddenly urged their followers to buy Bitcoin. Twitter only became aware of the issue after the sales pitch went out. Law enforcement got involved, and it turned out the criminals were... teenagers.

This story illustrates the dangers of private properties becoming public squares. What if the hackers are not teens but bad actors, even nation-states, seeking to propagate disinformation?

Analysis

The greatest differentiator, and where researchers placed some of the heaviest weightings, was the strength of 2FA methods and support for enterprise-grade authentication and authorization. Most consumers see 2FA as a single technology when, in truth, different levels of security with various 2FA options exist.

While platforms like Facebook and Twitter stand head and shoulders above TikTok, one thing they all have in common is that none of them offer mature, enterprise-grade security options outside of 2FA. Even in the category of 2FA, support for emerging standards like FIDO2 and U2F (passwordless) is inconsistent across social media platforms. **This is a massive challenge as a lack of enterprise-grade authentication options leaves political leaders susceptible to credential reuse attacks.**

U.S. politicians must manage their own passwords on these platforms and, hopefully, use 2FA. Suppose these platforms offered support for enterprise-grade authentication methods like SSO. In that case, politicians would no longer need to manage their passwords. They could rely on their armies of IT staffers via integrations with popular identity management solutions like Okta and Microsoft's Azure Active Directory. Unfortunately, researchers noted that Facebook is the only provider with enterprise-grade authentication partially rolled out to users.

Figure 1 shows the social media platform security ranking.

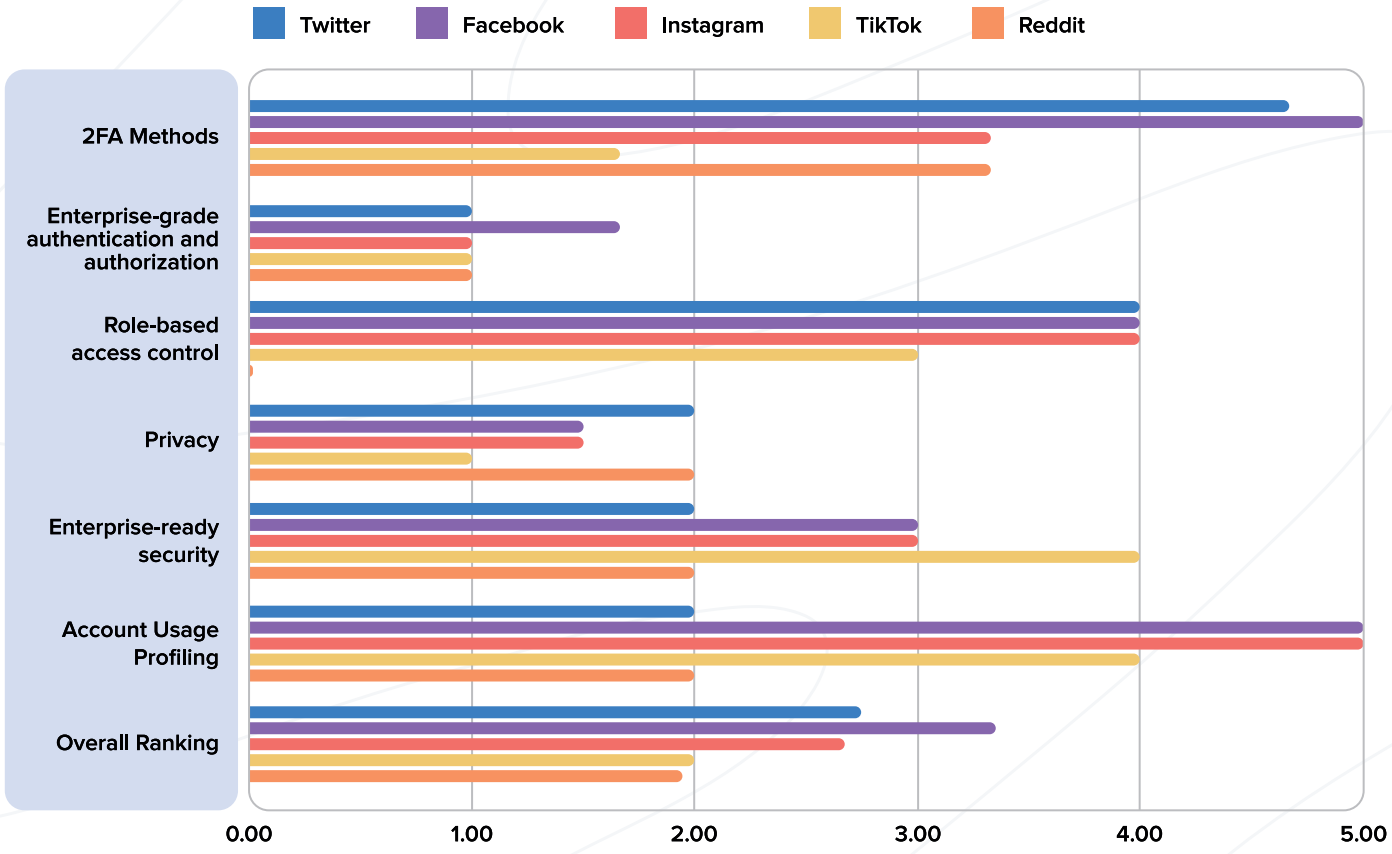


Figure 1. Social Media Platform Security Ranking

Scoring key

The following table describes the scoring key that researchers used to rate the security controls social media platforms offer.

Score	Description
0	No current support and no roadmap (publicly disclosed)
1	Roadmap item (publicly discolsed) or partial compensating control
2	Minimally supported (little to no maturity in category)
3	Partially supported (category is maturing)
4	Supported (category is supported but not fully mature)
5	Full support, mature

Table 1. Scoring Key

How to interpret the rankings

The following table describes what the researchers rated in every category.

Category	What was rated
2FA methods	SMS, TOTP, FIDO, FIDO2, U2F
Enterprise-grade authentication and authorization	SSO, SAML, SCIM, strong passwords
Role-based access control	Least privilege support
Privacy	Ability to limit data sharing and time-based third party application access grants
Enterprise-ready security	Openness of platform for programmatic access to platform security controls
Account usage profiling	Ability to profile account usage and lock down account in case of unusual usage

Table 2. Rating Criteria

Influencing a vote is much easier than directly changing one in an election system—at least in the U.S. Every nation-state has an unquenchable appetite for data. Consider that the U.S. has been the biggest data requester for many of the most popular social media platforms. Don't think of one social media platform's data in isolation, but what could a nation-state do with it in conjunction with data from public and dark web sources—like the Twitter breach in 2022 that exposed millions of its users? Any nation-state with access to this volume of data could use it in the following real-world scenarios:

- Develop targeted campaigns to identify those with access to sensitive intellectual property and execute spear-phishing campaigns to gain access. For example, someone working for a defense contractor or telecommunications company could be a prime target.
- Sway the opinion of a group of users by promoting a certain point of view advantageous to the geopolitical fortunes of the nation-state and its allies. This would likely be done via the algorithm that recommends videos or posts.
- Create a long-haul campaign to uniquely identify individuals they predict will have the most future influence in industry or society. Predictions can be based upon various degrees of separation, among other factors. These individuals could be targeted and influenced for years and may eventually be approached for espionage purposes.

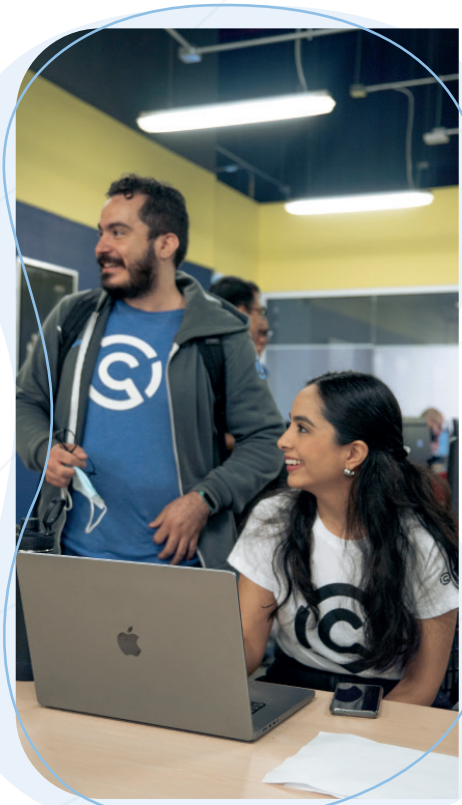
Disinformation works best when a nation-state can coordinate its efforts across multiple platforms. Politicians need to look at these findings through two lenses: the social media platforms' security and the level of security controls the platforms offer to politicians as end users. *Importantly, researchers highlighted that each platform has a high development velocity, meaning that the security and privacy features they offer change rapidly and at any time.*

No surprises

Despite their continued growth as the news medium of choice for voters, the U.S. does not have security standards or oversight for social media platforms. Until this changes, politicians and voters should expect a continued assault from nation-states looking to execute disinformation campaigns.

Nearly every social media platform lacks enterprise-grade authentication options. This is a travesty for not only politicians but also businesses across the globe that rely on them to communicate with consumers. Social media platforms fall into an emerging category called “unmanageable applications.” Most enterprise-ready applications offer support for common security standards like single sign-on (SSO/SAML) and have features that security and IT teams can plug into their existing security tools. Unmanageable applications offer none of these options, yet most employees and politicians continue to use these applications without the oversight of IT and security teams.

What are unmanageable applications?
Unmanageable applications are those that do not support industry standards like SAML for authentication and SCIM for automatically adding and removing users from applications.



Guidance

Political leaders must ensure they use solid passwords via a password manager and have the most powerful 2FA method enabled. They should not use SMS-based 2FA as it is easy to exploit and a favorite of attackers. On Facebook and Twitter, this means using something like a YubiKey to take advantage of the ultra-secure emerging FIDO2 standard. On platforms like TikTok, unfortunately, they are relegated to email-based 2FA or, worse yet, SMS-based 2FA, which is very susceptible to SIM-based attacks.

Political leaders with IT staffer support and SSO providers available (for example, Okta and Azure Active Directory) should consider emerging options that allow connecting social media platforms, such as those reviewed in this brief, even if they lack native support.

Researchers note that a delicate balance exists between too little and too much regulation. In the digital realm of the U.S., free speech online is regulated by Section 230 of the Communications Decency Act, which went into law in 1996. Politicians need to consider updating this regulation to provide security and privacy oversight for social platforms that now dominate the U.S. political landscape.

Methodology

Researchers evaluated Twitter, Facebook, Instagram, TikTok, and Reddit in late 2022 using a scale of 0 to 5 (detailed in the Analysis section of the briefing). Researchers evaluated each platform across six categories and assigned a weighting to each: 2FA methods (30%), enterprise-grade authentication and authorization (25%), role-based access control (10%), privacy (15%), enterprise-ready security (10%) and account usage profiling (10%). All data were summarized by category and not by individual technology, such as FIDO2 support or a lack of SCIM support. Certain platforms offer business versions; in some cases, researchers also factored these into their scoring. For example, researchers attempted to identify where a political candidate might use enterprise features vs. the standard consumer offering.

2FA methods
30%

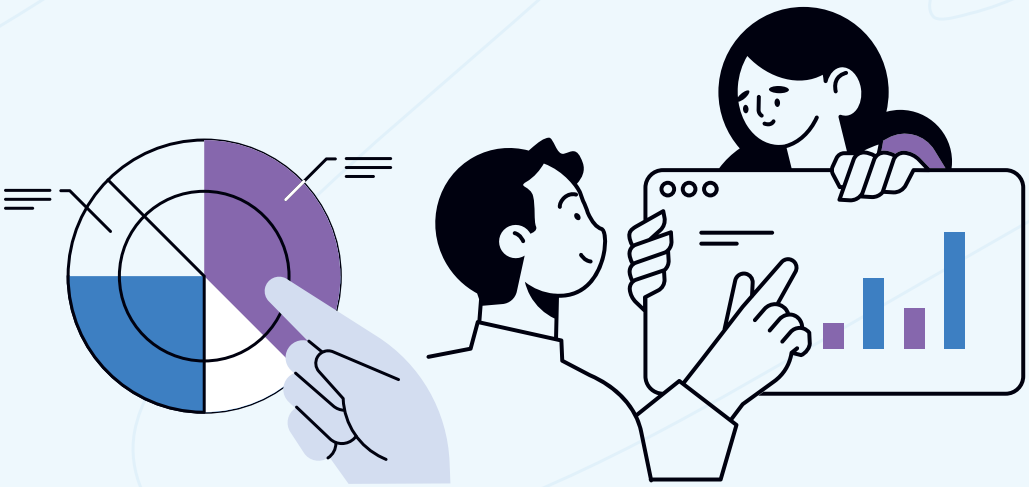
Enterprise-grade authentication and authorization
25%

Role-based access control
10%

Privacy
15%

Enterprise-ready security
10%

Account usage profiling
10%



cerby®