cerby®

Threat Briefing: Social Media Security and Elections

Volume II

Table of Contents

Executive Summary

Despite the media coverage afforded to social media platforms' security and privacy, our research indicates a multi-year gap in their support for enterprise-grade authentication and authorization. For political leaders and businesses, the ability to tie social identities to corporate credentials is critical in preventing account takeovers and misinformation. Furthermore, most high-profile political leaders do not manage their social presence but rely on an army of staffers. Without enterprise-grade authentication and authorization, usernames and passwords are shared, and two-factor authentication (2FA) is disabled, a high-risk combination often leading to account takeovers.

More clarity is still necessary around best practices for businesses and political leaders to secure their accounts. However, as social media platforms cement their role in democratic discourse in the US, ensuring their security is paramount, especially with the November 2023 US elections.

We assessed five platforms—Facebook, Twitter, Instagram, TikTok, and YouTube—across six key security parameters on a scale of 0 to 5, with 0 meaning they don't support security controls or don't have a public roadmap to implement them and 5 meaning they fully support them and the controls are mature. This year, we added YouTube and removed Reddit, aligning the evaluation with the current top social media platforms. The average score across all platforms and parameters slightly improved from 2.54 in 2022 to 3.02 in 2023, marking an 18.9% enhancement. For the second year in a row, Facebook took the top prize with an overall score of 3.74. YouTube came in second at 3.15. Taking the third spot was Twitter with 2.95, followed by Instagram at 2.78, and TikTok at 2.5. However, this progress doesn't translate to a substantial mitigation of risks, especially with the upcoming elections.

Based on the findings, researchers at Cerby are not recommending politicians and businesses avoid using these platforms but focus their efforts on platforms scoring at least 2.6 or higher.

Figure 1 shows the overall ranking of each social media platform for 2023.

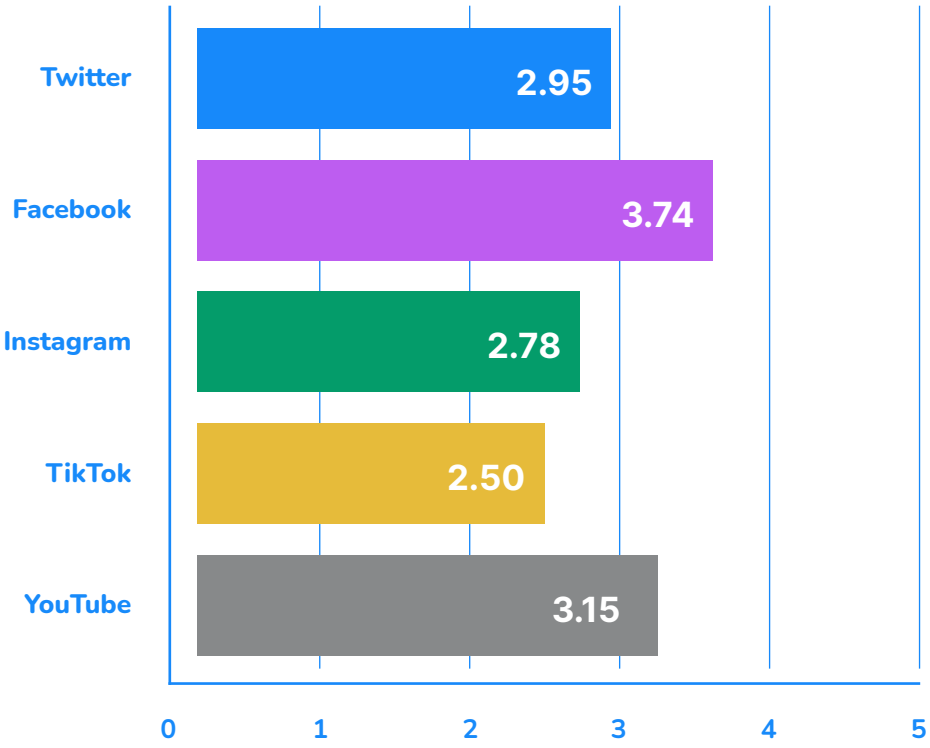

Figure 1. Overall Scores For 2023

Key findings

The following are some of the key findings regarding security and privacy controls on the social media platforms:

Two-factor authentication (2FA)
Twitter significantly improved 2FA by supporting the phishing-resistant FIDO2 standard (a global authentication standard based on public key cryptography), scoring a perfect 5–joining the ranks with Facebook and YouTube.

Enterprise-grade authentication and authorization
The category saw no change from last year. This finding highlights a glaring security gap and low adoption of vital standards such as SAML for authentication (single sign-on or SSO) and the System for Cross-domain Identity Management (SCIM) for automated user access onboarding and offboarding. Both are critical controls for protecting against account takeovers and individuals retaining access to high-profile accounts after they leave an organization.

Privacy controls
An average increase of 25% was noted, primarily driven by Facebook's significant improvements. Facebook leaped from 1.5 to 3.5 due to solid enhancements, specifically with time-based third-party access—an essential safeguard against retained access.

The year-over-year comparison reveals a commendable advancement in 2FA methods, a positive stride towards securing user accounts. However, **the stark need for enterprise-grade authentication and authorization is concerning**. This lack of integration leaves political and business leaders vulnerable to credential reuse attacks and account takeovers, which can lead to disinformation, particularly during elections.

The data underscores a pressing need for a collaborative effort between political leaders, enterprises, and social media platforms to integrate social identities with enterprise identities managed by identity providers like Okta and Azure Active Directory (Entra ID). Addressing this security void as the election dates inch closer is imperative to ensure a secure digital environment for robust democratic engagement. The onus is on political and business leaders to push for a more integrated and secure social media ecosystem, aligned with enterprise-grade security standards to mitigate the risks posed by the current controls offered by social media platforms.

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.

fido™

Analysis

High-profile account takeovers, like the Twitter Bitcoin scam in July 2020, show the potential risks when attackers gain unauthorized access to significant accounts. This incident saw prominent accounts, including those of Elon Musk and Barack Obama, hijacked to promote a Bitcoin scam. With incidents like these happening frequently, the cornerstone of our assessment remains the robustness of 2FA methods and the support for enterprise-grade authentication and authorization. The common misconception, especially among business and political leaders, is that 2FA is a monolithic technology. However, its security level varies greatly depending on the specific 2FA method, for example, SMS vs. time-based one-time password (TOTP, such as Google Authenticator) vs. FIDO2.

Figure 2 shows how each social media platform's security ranking changed year over year.
Note: For consistency, all year-over-year comparison charts exclude YouTube (not assessed in 2022) and Reddit (not assessed in 2023).

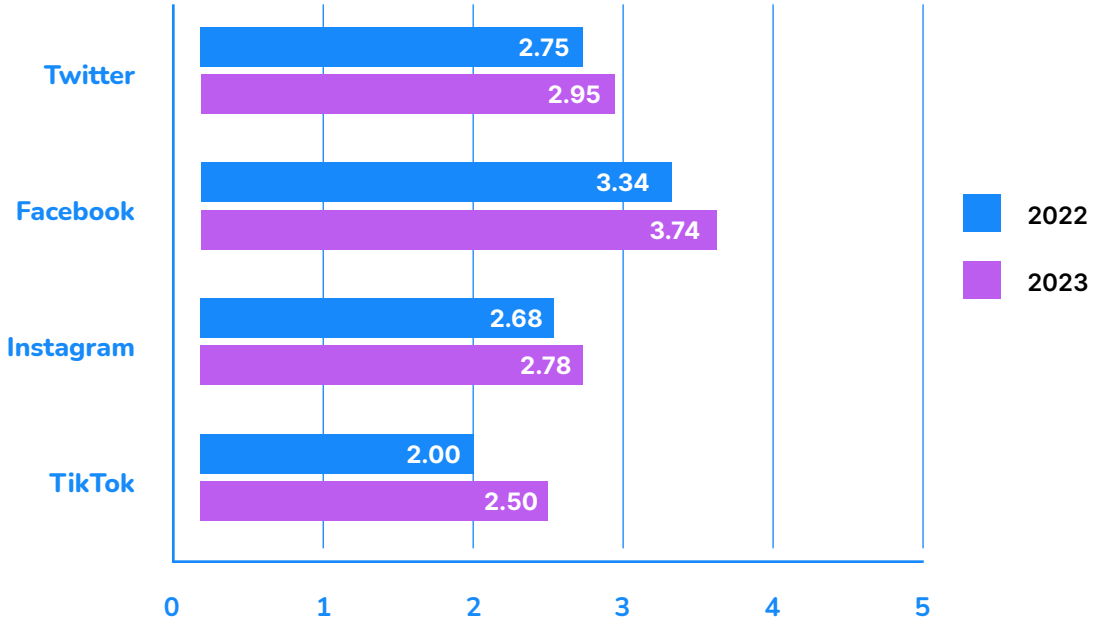

Figure 2. Overall Scores Year Over Year

The year-over-year analysis unveils a discernible improvement in 2FA across multiple platforms. Noteworthy is Twitter, improving its score by 7.1% to a stellar 5 in 2023 from 4.67 in 2022, thanks to its adoption of the phishing-resistant FIDO2 standard. YouTube, a newcomer to our study, made an impactful entrance with a 5 score in 2FA methods, displaying a solid commitment to user-centric security measures. TikTok also displayed a positive leap, doubling its score to 3.33 from 1.67 by incorporating TOTP support across business and personal offerings. This advancement reflects the platforms' responsiveness to escalating security concerns and their endeavors to bolster user trust.

Figure 3 shows the overall change in 2FA scores from 2022 to 2023.

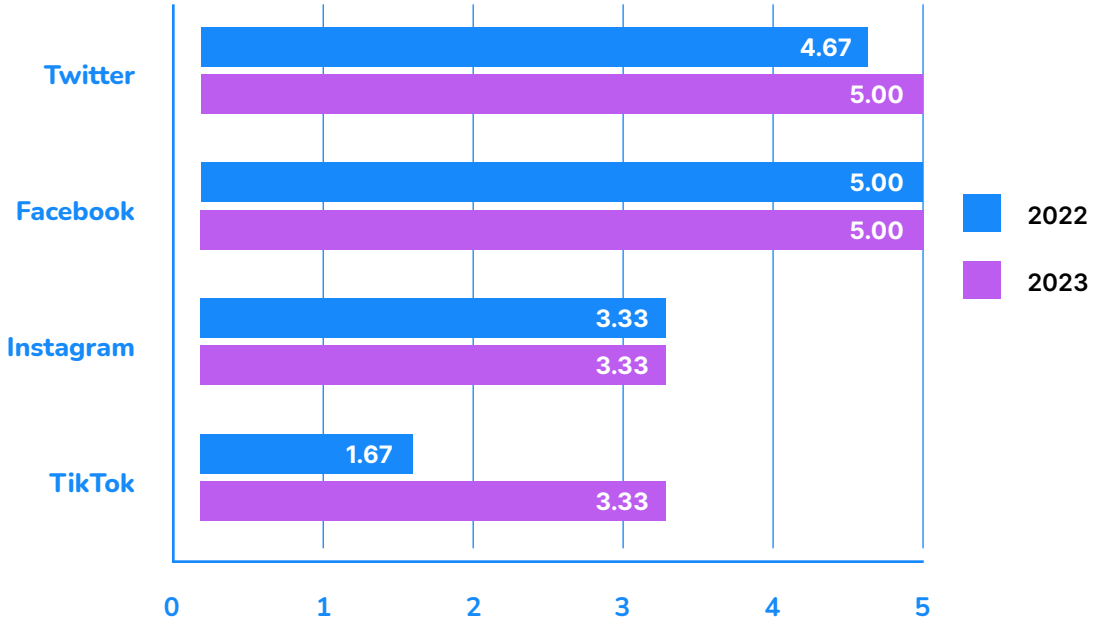

Figure 3. 2FA Scores Year Over Year

However, the Achilles' heel across most platforms is a lack of support for mature enterprise-grade authentication and authorization, particularly the SAML and SCIM standards. **Without these standards, political figures and businesses are vulnerable to several security risks, including credential reuse attacks.** This area saw no remarkable improvements, stagnating at a score of 1.13. The unchanged nature of these scores from 2022 to 2023 highlights a misalignment concerning enterprise-grade security controls within these platforms.

While diligent password management and 2FA utilization are advised, the most comprehensive solution is integrating social identities with enterprise identity management solutions like Okta and Microsoft Azure Active Directory (Entra ID). Doing so allows businesses and politicians to move away from managing passwords and 2FA codes for each social network to using a single corporate identity across multiple social platforms.

Figure 4 shows the overall change in privacy scores from 2022 to 2023.

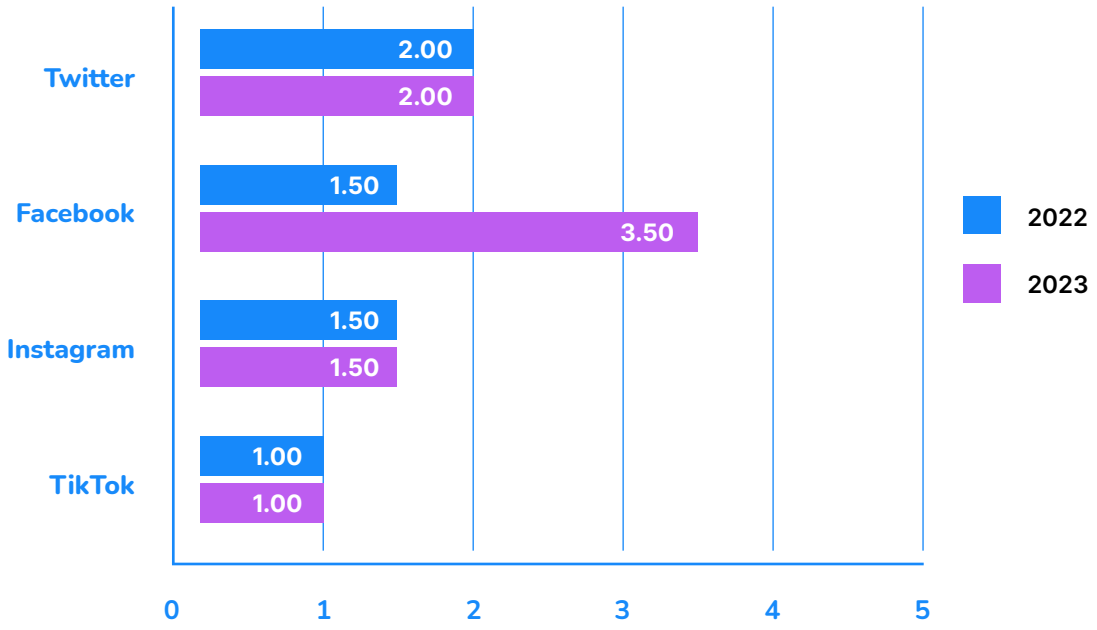

Figure 4. Privacy Scores Year Over Year

The persistently low scores for enterprise-grade authentication and authorization across many platforms signal a red alert as we inch closer to the crucial US midterm elections in 2023 and the EU Parliament elections in 2024.

Figure 5 shows the overall social media platform security ranking for 2023.

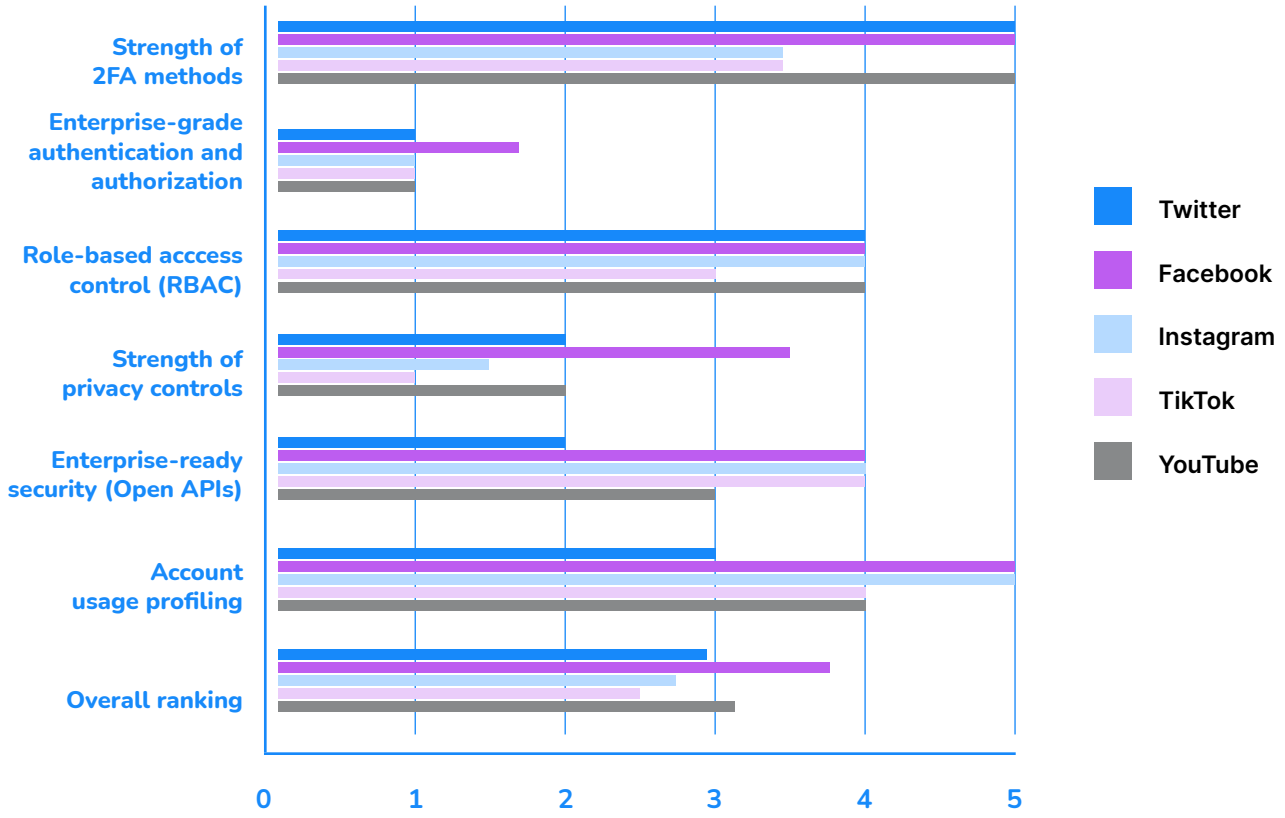

Figure 5. Social Media Platform Security Ranking for 2023

Scoring key

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

Score	Description
0	No current support and no roadmap (publicly disclosed)
1	Roadmap item (publicly disclosed) 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 (RBAC)	Least privilege support
Privacy	The ability to limit data sharing and time-based third-party application access grants
Enterprise-ready security	Openness of the platform for programmatic access to platform security controls
Account usage profiling	Ability to profile account usage and lock down accounts in case of unusual usage

Table 2. Rating Criteria

What are nonstandard applications?

Nonstandard applications (sometimes called decentralized applications) do not support industry standards like SAML for authentication and SCIM for automated user onboarding and offboarding from applications, posing significant risks in a data-driven ecosystem.

Future Outlook

The significant need for progress in enterprise-grade authentication and authorization across social platforms remains challenging. These platforms broadly fall into the nonstandard application category, needing more support for common security standards like SAML and SCIM, leaving politicians and businesses adrift in turbulent waters with minimal oversight from IT and security teams.

The recent enactment of the UK's Online Safety Act is a testament to the pressing global necessity for heightened security measures on social platforms. This legislation, while primarily focused on content moderation and user safety, hints at a larger narrative of fostering a secure digital environment, which invariably circles back to robust authentication and authorization mechanisms. It sets a precedent that may ripple across the pond, influencing legislative agendas as we approach the US midterm elections in 2023 and the EU Parliament elections in 2024.

Guidance

In light of the new findings, it remains imperative for political leaders and businesses to fortify their online presence against the escalating threats that lurk within the social media landscape. The protective measures encapsulated below are instrumental in bolstering security amidst the storm of cyber adversities:

1

Robust password management
Using password managers integrated with corporate identity providers is crucial to ensure the creation and safe storage of complex passwords, minimizing the risks associated with weak or reused passwords.

2

Enhanced 2FA

- It's pivotal to employ the most robust 2FA methods available. On platforms like Facebook, Twitter, and YouTube, leveraging hardware-based security keys, such as a YubiKey, is advisable to attain a higher security posture.
- TikTok, which still lags in offering advanced 2FA options, needs more cautious engagement. Political leaders and businesses are urged to use authentication apps like Google Authenticator (TOTP).

3

Enterprise integration
For political leaders with access to IT support, integrating social media platforms with enterprise SSO solutions like Okta or Microsoft Azure Active Directory (Entra ID), even without native support, is prudent. This approach facilitates a centralized and more secure management of access credentials, thereby bolstering overall security.

Methodology

Researchers evaluated Twitter, Facebook, Instagram, TikTok, and YouTube in late 2023 using a scale of 0 to 5, as detailed in the **Analysis** section of this briefing.

Each platform was assessed across six categories, each with its weighting: 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%). The data were summarized by category, not by individual technology like FIDO2 support or the absence of SCIM support.

The change from last year includes adding YouTube and removing Reddit, aligning the evaluation with the current top social media platforms. In some instances, researchers also considered the enterprise versions of these platforms to understand the potential security posture for political candidates using enterprise features versus standard consumer offerings.

About Cerby

Cerby provides identity teams with the only comprehensive access management platform for nonstandard applications. Harnessing the power of identity providers, Cerby removes the need for manual tools and compensating controls (like enterprise password managers) by automating everyday human security tasks based on single sign-on and lifecycle management cues from upstream identity providers. This allows Cerby to protect any application independent of standards support. Cerby's patent-pending access orchestration engine is the first and only one to make passwordless authentication an immediate reality for nonstandard applications. Cerby saves time and money by automating manual tasks, like offboarding and 2FA enrollment, and providing IAM professionals with deep visibility and control of employee-onboarded applications. With Cerby, identity teams can extend access, minimize risk, and lower costs.

Since we released our offering in 2022, Cerby's platform has enabled clients like L'Oréal, Fox, Colgate-Palmolive, Dentsu, and Televisa to detect nonstandard apps and guide business users to more secure alternatives, all while keeping everything under the umbrella of their identity provider.

Visit us at Cerby.com and follow us on social at @CerbyHQ.