Social Media and the Shared Privileged Account: Preventing Costly Account Takeovers

Solution Brief
Social media is playing an increasingly important role in an enterprise’s marketing strategy – and for good reason. Social media can help build brand awareness, provide a new level of customer support, and launch new products quicker than ever before.

However, social media also poses a costly security risk. As hackers become more sophisticated, they are becoming adept at stealing social media credentials and taking over accounts, as witnessed by hacks of several large corporations over the last year. Account takeovers can lead to the unauthorized publishing of confidential information, such as intellectual property, legal, regulatory, and compliance violations, disclosure of personal data, and identity theft. The result can be severely compromised brand reputations and significant financial loss.

With more frequent attacks of this nature, it's time for organizations to take a closer look at how they manage their social media accounts. And it's imperative that they take measures to prevent hackers – as well as disgruntled employees or associates – from hijacking accounts and posting damaging content.

**Social Media Hacks Are on the Rise**

When a corporate social media account is compromised, unauthorized content can be viewed by millions of people across the world within seconds, causing untold damage.

For instance, in April of 2013, hackers (supposedly from the Syrian Electronic Army) got into the Associated Press (AP) Twitter account. A single tweet resulted in a $136.5 billion drop in the S&P 500 index’s value in minutes. The AP was able to trace the attack to one of its employees that may have inadvertently given away company passwords in a “phishing” scheme by hackers.

Burger King’s Twitter account was compromised earlier in the year. During the hack, the company’s Twitter account was made to look like McDonald’s with a post that said Burger King had been sold to McDonald’s. This attack served as a wakeup call for all organizations that hackers are on the prowl for access into social media accounts. In fact, a day after the Burger King incident, a similar attack – possibly by the same group behind the food chain’s attack – occurred on the official Twitter page for Jeep, citing that the company was sold to Cadillac.

The above hacks were caused by external groups, but there can be equally damaging incidents caused by people inside an organization that at one point were given authorized access to a company’s social media accounts. This happened to HMV, an entertainment retailer based in the UK, after the company let go a large number of employees. One disgruntled laid-off employee, who was formerly HMV’s social media manager, took advantage of her access to the company’s Twitter account before officials realized she still had access. Her unauthorized post called attention to what she labeled as the company’s “mass execution of loyal employees who love the brand.”

---

The Overlooked Threat: Shared Privileged Accounts

One reason it is so easy for hackers to hijack social media accounts is because of the sheer volume of accounts of this type and the large number of people managing them.

Enterprises have hundreds of social media accounts on Twitter, Facebook, YouTube, LinkedIn, and other outlets with unique accounts for different product lines, languages, countries, and stakeholders (such as consumers, partners, and stockholders).

These accounts are typically set up as shared privileged accounts, meaning that teams of people throughout an organization can post information to these accounts on a daily, hourly, or even more frequent basis. The passwords for these are often shared among the teams, making them easy targets for hackers and malicious insiders. In addition, there is no record or accountability for each individual’s posts, leading to further challenges in securing and managing social media accounts.

Because people posting on social media accounts don’t typically have access to financial or customer information that is traditionally deemed of high value, the security on these accounts is often lax, with little management and control of the passwords. In fact, companies may not even know who has access to their social media accounts or the passwords on the accounts. To make matters worse, the same password is frequently used across multiple accounts, and the passwords are rarely changed.

Lax security also opens the door for rogue current or past employees (as seen in the HMV example) or social media agency members that are disgruntled. And, hackers are becoming more sophisticated – and more organized. They can essentially comprise any system that is lacking proper security as they use multiple methods of intrusion including dictionary attacks, social engineering, software, or social media applications. For instance, the use of Twitter and Facebook accounts can introduce additional risks, as these platforms may provide hackers with access to valuable data such as passwords, APIs, or other sensitive information.
Mitigate the Risk of Social Media Breaches

Social Media Management Systems are often adopted by organizations to manage social media accounts, but these solutions are built as management tools and lack a focus on security. These solutions leave organizations vulnerable due to the continued use of static passwords and multiple users. In order to properly secure and protect social media accounts, they should be viewed as privileged accounts and best practices for privileged account security must be employed to mitigate the risk of compromise.

The following preventative measures must be adopted to secure Social Media account access and protect an organization’s brand.

- **Securely store credentials:** Protect social media credentials from being stolen by storing passwords for the accounts in a secure place, such as the CyberArk patented Digital Vault™. This will reduce the ability of hacker organizations to take over social media accounts.

- **Enable transparent access:** Allow authorized users to seamlessly authenticate to the account without knowing their passwords, making it difficult for hackers to discover and steal credentials. Utilizing an agent-less technology securely exchanges passwords without requiring an agent on the cloud applications.

- **Eliminate shared credentials:** Storing passwords in a digital vault requires users to login individually for access, eliminating the accountability challenges of shared credentials.

- **Automate and enforce password changes:** Ensure that each password is changed on a regular basis. Passwords can be changed as frequently as after every use. Regularly updating passwords reduces the chance of an outsider stealing and using a valid credential.

- **Trace account activity:** Create a record of activity on social media accounts to trace all posts directly back to an individual authorized user. This helps identify weak areas of security and identifies rogue employees that may be posting damaging content.

- **Record social media sessions:** Record social media account sessions, providing further proof and an audit trail of exactly who did what within an account.

The threat to social media is real, it’s evolving, and the risk is increasing. Preventing account takeovers through shared privileged accounts is imperative and necessary. Privileged Account Security solutions from CyberArk play a critical role in protecting access to social media accounts thereby preventing embarrassing incidents that can result in brand damage.
About CyberArk

Enterprise-Proven, Industry-Leading Experts

With our award winning, patented technology and proven expertise, CyberArk is the only security company laser-focused on striking down targeted cyber threats. And we are the only company that can provide full protection from advanced and insider threats to mitigate your risks and meet high stakes compliance requirements.

Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world’s leading companies – including more than 35 of the Fortune 100 – to protect their highest-value information assets, infrastructure, and applications. We have more deployments in large-scale distributed and virtual environments, solving more privileged account security challenges than any other vendor. We can support any device, any data center, for on-premise, hybrid cloud, or OT/SCADA environments. CyberArk is the only vendor with a native solution that can provide full protection, monitoring, detection, and reporting of privileged accounts.