



Tips for Keeping Corporate Social Media Accounts Secure



**HERE ARE SOME EYE-OPENING
STATISTICS THAT HIGHLIGHT JUST
HOW FAR SOCIAL MEDIA HAS COME**

A long time ago — but in this galaxy vs. one far, far away — something strange called social media arrived on the scene. At first, it was generally viewed by businesses with scorn and skepticism. But soon, it became clear that social media was a tool, not a toy.

The Growth of Social Media

Here are some eye-opening statistics that highlight just how far social media has come since those early days of ICQ, Friendster and good ol' MySpace:

- [97% of digital consumers](#) have used social media in the past month.
- [84% of people with access to the internet](#) use social media.
- [50% of the global population](#) now uses social media.
- In 2019, the average social media user spent [2 hours and 24 minutes on social media each day](#).
- The average social media user has [8.3 different accounts](#).

Rise in Social Media-Based Cyber Crime

However, the surging popularity of social media across the business landscape isn't entirely positive, because it has led to a massive rise in cyber crime. Here are some of the grisly numbers:

- [22% of social media users](#) said that their online accounts have been hacked at least once, while 14% reported they were hacked more than once.
- Fraud attacks on social media [increased by 43%](#) between 2017 and 2018.
- The data of [more than 1.3 billion social media users](#) has been compromised within the past 5 years.
- Up to [40% of social media sites](#) have some form of turn-key hacking tools or services available for purchase.

Ironically, the same thing that makes social media so popular is also what makes it so dangerous: the belief that people are communicating with people they know — or at least, communicating with people who won't try and hack their device and steal their identity. As pointed out by the [New York Times](#): "The human error that causes people to click on a link sent to them in an email is exponentially greater on social media sites... because people more likely consider themselves among friends."

User-Focused Best Practices for Keeping Social Media Accounts Secure

If you're an IT pro, then you probably don't need to discover best practices for keeping your social media

accounts secure — because you're already following them (although a little reminder never hurts, right?). However, there's a good chance that some, many, or possibly most, of your non-technical colleagues aren't as committed to or concerned about social media security. This neglect or indifference doesn't just put them at risk: it puts the entire company at risk.

And so, in an effort to close that gap, here are some social media security tips that we encourage you to share with your colleagues, and even your clients/customers:

- Never click on suspicious messages or links, even if they seem to be posted from someone you know. Instead, flag these posts for investigation.
- Never post any personally identifying information (PII) that may allow cyber criminals to guess your password or security questions (e.g. name of your first pet, name of your high school, etc.).
- Only use unique, strong passwords or passphrases for each of your social media accounts. An estimated [81% of data breaches](#) are due to weak passwords.
- Use a good password manager instead of writing down/storing your login credentials.
- Never share passwords with colleagues, friends or family members.
- Always use [multi-factor authentication](#) for each of your social media accounts.
- Avoid logging into social media accounts while using a public Wi-Fi access point. If this is impossible, then use a good VPN to encrypt your data and protect your identity.

Company-Focused Best Practices for Keeping Social Media Accounts Secure

In addition to the above steps, there are some key things that companies should also do, in order to reduce the risk of social media-related cybercrime. If you're doing all of the following, then give yourself a pat on the back. If you aren't, then consider adding them to your priority list and making them happen ASAP:

- Implement a comprehensive social media usage policy that clearly establishes acceptable behavior/actions. This should include a system to review and approve/reject posts made to company social media accounts.
- Limit social media access per the [Principle of Least Privilege](#) (POLP).
- [Screen proposed social media account passwords](#) against lists of known compromised passwords.
- Provide social media training, preferably through an [online cybersecurity training platform](#) that allows

end users to learn independently, and at the same time allows managers to track progress and identify knowledge gaps.

- Use smart technology like [Devolutions Password Hub](#) that makes it easy and secure for end users to create, vault, and (if necessary) share group passwords, or provide access to specific social media accounts (but without revealing credentials).
- Regularly audit social media privacy settings, access and publishing rights, and recent social media security threats.

From the Desk of Our CSO Martin Lemay:

Social media risks are often overlooked by organizations, either because they do not consider them harmful to the brand or they don't realize all the threats surrounding their landscape. While all the best practices stated above are good to apply, they will mostly protect your social media accounts, and not your brand or your corporate infrastructure.

User and brand impersonation could target your employees, partners and customers without having to hack any corporate account. Just like a phishing e-mail from your not-so-legit favorite banking institution, a social media account could perform similar attacks to not only deceive other users, but also to damage your reputation. There are services available for social media brand monitoring that will automatically look for such attacks on all social media platforms and take rapid action to take compromised accounts down. Those services also often include phishing and vishing protection and rely on threat intelligence sources to detect active attacks against your brand.

Another common threat is malware delivery through social media platforms. Your organization might have deployed that fancy anti-spam/anti-phishing platform with automated sandboxed malware analysis and protection. Or it might prevent dangerous document types from getting through. However, if a malicious document or application is downloaded through a social media platform, it has just bypassed all this fancy (and costly) stuff. Now you have to rely on your endpoint protection software to catch that potentially devastating malware. Make sure your defensive strategy includes that risk not only on corporate computers, but also on portable devices such as phones and tablets that are authorized in the organization's environment.

Social media is and should be considered an attack vector that requires the same attention as any other attack vector in your environment. Do not overlook that threat. Stay safe.