KEEPER
Cybersecurity Starts Here™

Social Media Security Best Practices

How to Protect Your Social Media Passwords from Cybercriminals

TABLE OF CONTENTS

BACKGROUND

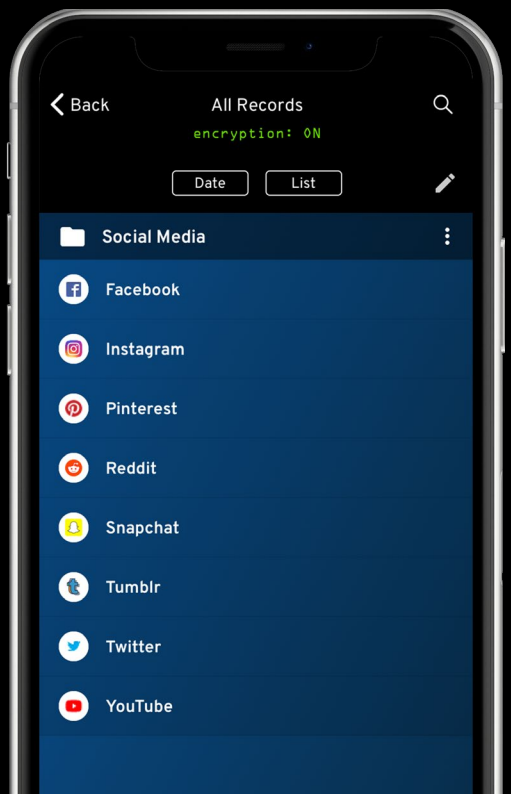
All businesses, regardless of size or industry, are potential targets for cybercriminals. A study of global small and medium-sized businesses (SMBs) conducted by the Ponemon Institute in conjunction with Keeper Security found that 66% of respondents had experienced a cyberattack over the previous 12 months, and 72% had been attacked within their companies' lifetime.[1] Meanwhile, over 80% of successful data breaches can be traced back to a stolen or compromised password.[2]

As businesses become more aware of the importance of password security in preventing data breaches, they focus on the most obvious areas of weakness, such as employee email accounts and network passwords. However, social media passwords present unique security challenges that organizations may be ill-prepared to handle.

This lack of proper password security is particularly vexing for social media and digital marketing agencies, which handle multiple clients that include companies and high-profile individuals, such as social media influencers and celebrities. However, marketing departments at large enterprises or SMBs encounter similar problems with securing their companies' social media passwords.

In this paper, we will examine these challenges, then discuss how implementing a password management solution can help overcome them.

MANY COMPANIES DON'T PROPERLY SECURE THEIR SOCIAL MEDIA PASSWORDS



A lack of centralized social media password management leaves organizations vulnerable to cyberthreats; at social media agencies, the vulnerabilities begin during the client onboarding process.

- Typically, clients insecurely share their social media passwords with their agency, through unencrypted email or text messages, which can be intercepted by cybercriminals.
- The client may store passwords in a spreadsheet or text file, which creates a single point of failure; if this document is compromised, all of the client's accounts are compromised.
- The client may use the same password for all their social media accounts, ensuring that if a cybercriminal gets hold of that password, they can access every account.
- The client's passwords may be weak or they may have already been compromised in a public data breach, leaving the accounts vulnerable to credential-stuffing and password-spraying attacks.

Once the agency has a client's credentials in-hand, they too share and store them insecurely, in a shared spreadsheet or text file, on sticky notes, or through unencrypted email or text messages. Some agencies may even store all client credentials in one "master list."

Typically, business social media accounts are managed by teams that include administrative personnel, designers, copywriters, and other marketing and public relations specialists. Team members may consist of in-house employees, freelance contractors, or a combination of both. The more people who have access to an account's login credentials, the bigger the risk that those credentials will be compromised. Verizon estimates that 57% of data breaches involve careless or malicious acts by a company insider, and 15% of data breaches are caused by intentional misuse of login privileges by workers or contractors.[3]

A lack of centralized social media password management raises the insider threat level. Individual employees and contractors may store client credentials in their web browsers or create their own spreadsheets, text files, or sticky note collections. When each team member has their own "system" for storing account passwords, the organization has no visibility into password usage by its employees or contractors, nor do they have a way to disable access when one of them leaves the company.

Without centralized visibility and control, account passwords are more likely to be compromised due to negligence, carelessness, and malicious acts by disgruntled current or ex-employees. It's also not feasible to secure accounts with two-factor authentication (2FA), which leaves accounts even more vulnerable to compromise.

THE POTENTIAL FALLOUT OF SOCIAL MEDIA ACCOUNT COMPROMISE

Agencies may have even more risk than account owners

Social media account compromise has been going on for at least a decade.[4] One study estimates that at least two-thirds of U.S. adults have had at least one social media account compromised,[5] while another states that up to 53% of social media logins are fraudulent.[6]

When an account belonging to a business or a high-profile individual is compromised, the ramifications can be severe. Once logged into the compromised account, cybercriminals can:

- Access personally identifiable information (PII) and other sensitive data, which they can use to blackmail the account owner or leverage for future social engineering attacks.
- Change the account settings and lock out the real owner, then demand a ransom to let the owner back in or, alternatively, sell the account on the dark web. Short, unique Instagram handles can fetch between $500 and $5,000.[7]
- Use the social media channel's direct message function to target account followers with malicious links, which is especially dangerous considering that many people trust direct messages sent to them by the people and brands they follow.
- Post spam or other malicious content to the account's public feed, which could damage the brand's reputation.

If the account is linked to an ad manager, cybercriminals can run malicious or embarrassing ads, all charged to whatever credit card is on file. After cybercriminals breached a Facebook account belonging to an employee at LiveRamp, a major Facebook data partner that helps advertisers target ads on the platform, they were able to access its Business Manager account and use it to buy and run ads for non-existent products. All of the phony ads, including one that was viewed more than 60,000 times, were paid for by other accounts' credit cards.[8]

Other high-profile social media account compromises include:

- In early 2020, the cybercriminal group OurMine breached social media accounts belonging to the NFL and 15 of its teams, posting embarrassing messages chiding the teams for their apparent lack of cybersecurity.[9]
- About a month after the NFL breaches, OurMine hijacked the official Twitter accounts of FC Barcelona, the Olympics and the International Olympic Committee (IOC); this was the second time in three years that FC Barcelona's social media feeds had been victimized by OurMine.[10]
- Even Facebook itself couldn't escape the wrath of OurMine, which breached the social media giant's Twitter accounts.[11]
- In 2019, after breaching comic Ellen DeGeneres' Instagram account, cybercriminals used the feed to post phony prize giveaways.[12]
- In 2013, cybercriminals breached the Associated Press' Twitter account and posted a phony message claiming that two explosions had occurred at the White House, injuring then-President Barack Obama. The AP quickly realized it had been breached and posted a retraction, but not before the fake tweets caused a brief stock market panic, with the Dow Jones dropping nearly an entire percentage point.[13]

SECURING SOCIAL MEDIA ACCOUNT PASSWORDS

Securing social media account passwords means taking the same precautions as securing other enterprise passwords, including:

- Mandating that all social media accounts be protected with strong, unique passwords.
- Sign up for a dark web monitoring service, such as Keeper BreachWatch for Businesses, that will immediately alert you if any account passwords show up for sale on cybercriminal forums.
- Never transmitting passwords through unencrypted email or text messages.
- Controlling employee and contractor account access through role-based access control (RBAC), in conjunction with the principle of least privilege.
- Mandating the use of 2FA on all social media accounts that support it.
- Prohibiting the use of spreadsheets, sticky notes, and other insecure methods of keeping track of passwords, and mandating the use of a password manager such as Keeper.

In addition to making it easy to secure social media account passwords, a robust password manager such as Keeper provides social media agencies and other enterprises with a world of time-saving and security-enhancing benefits, such as:

- Store, secure, and manage all company passwords, not just social media accounts.
- Automatically generate and store strong, unique passwords for every account.
- Complete visibility into employee and contractor password usage so that password security protocols, such as mandatory 2FA, can be enforced.
- Ensure compliance with CCPA, HIPAA, GDPR, and other industry and regulatory mandates.
- Enhance employee productivity by eliminating the need to keep track of passwords and reset lost or forgotten passwords.
- Quickly terminate account access when an employee or contractor leaves the company.

WHY KEEPER?

Not all password managers are created equal. Some are more difficult to set up and maintain, particularly when integrating them with SSO or 2FA.

Keeper's business and enterprise password management solutions help thousands of companies all over the world prevent password-related data breaches, improve productivity and enforce compliance with industry-leading features such as:

Exclusive, proprietary zero-knowledge security architecture

Three-in-one solution for small businesses; use Keeper as your password manager, SSO and PAM solution

Ease of use for both IT admins and end users; rapid deployment on all devices with no upfront equipment or installation costs

Personalized onboarding and 24/7 support and training from a dedicated support specialist

Support for RBAC, 2FA, auditing, event reporting and multiple compliance standards, including HIPAA, DPA, FINRA and GDPR

Easy integration with SSO; no need for separate logins

Secure storage for sensitive files, documents, photos and videos on unlimited devices

Private vaults for each employee, plus shared folders, subfolders and passwords for teams

Complete flexibility; whether your organization is a tiny startup or a multinational enterprise, Keeper scales to the size of your business

ABOUT KEEPER

Keeper Security, Inc. ("Keeper") is the market-leading, top-rated cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards.

Named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and the InfoSec Award for Best Product in Password Management and for SMB Cybersecurity, Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM). Learn more at **https://keepersecurity.com.**

G2 Crowd
2020 Enterprise Leader
4.7 out of 5 stars

PCMag
Editors' Choice
4.5 out of 5 stars

App Store
Top-Rated Productivity
4.9 out of 5 stars

Google Play
Over 10 Million Installs
4.6 out of 5 stars

Gartner peerinsights
4.9 out of 5 stars

spiceworks
5 out of 5 stars

Trustpilot
4.7 out of 5 TrustScore

GetApp
4.7 out of 5 stars

Sources:
[1] Ponemon Report [2] Verizon Report [3] Insight Dice [4] TechNewsWorld [5] University of Phoenix [6] Arkose Labs
[7] MarketWatch [8] SC Magazine [9] ZDNet [10] WeLiveSecurity [11] Business Insider [12] Deadline [13] MarketWatch