

FEBRUARY 13, 2026 | PUBLICATION

Protecting Your Business' Social Media Accounts from Hackers

For small and medium-sized businesses, social media platforms like Facebook and Instagram are essential marketing tools. However, account takeovers by hackers pose a serious and growing threat that every business owner should understand.

Preventive Security Measures

Protecting your accounts begins with good security practices.

- Turn on two-factor authentication for all your business accounts to add an extra verification step beyond just your password.
- Regularly update your passwords, ideally every 90 days, using strong and unique combinations for each platform.
- Keep a close eye on your accounts for any suspicious activity, such as unfamiliar posts, login locations, or changes to account settings you didn't make. For instance, be cautious if you receive password reset emails you didn't request or if customers report receiving unsolicited messages from your account.

Hackers often exploit compromised business accounts by sending phishing messages, like fake promotions claiming winnings or urgent requests to verify payment details. Detecting issues early can help prevent serious problems.

The Risks of Platform Dependence

Relying heavily on third-party social media platforms can be risky. If hackers take over your account, you might lose direct contact with your customers and marketing channels. Platform recovery processes can be slow and frustrating, meaning your business could be left without its main way of communicating for days or even weeks. It's a good idea to diversify your online presence and keep an email list as a backup method of reaching your customers.

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Douglas A. Cherry

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Responding to an Account Takeover

If your account is compromised, act immediately. Attempt to reset your password and use the platform's recovery tools to regain access. Be sure to report the hack directly to the social media provider using their official help channels. Usually, following their reporting steps carefully and clearly is the best approach. Remember, your report might be reviewed by artificial intelligence, so sticking to the requested format is important. Being overly verbose or sharing unrequested materials may be detrimental. Alert your followers on other platforms or using back-up methods if your account has been compromised and keep a record of any suspicious activity in case you need to take legal steps later.

Beware of Follow-Up Scams

A critical warning: recently, we've seen some hackers voluntarily return access to client accounts. However, they do this in an effort to set up another scam. Shortly after the return, the hacker then pretends to be the social media provider by reaching out to ask for payment for "account protection" or "security services" to ward off any future hacks. Remember, trustworthy platforms will never ask for money in this manner. If you receive such a message, please report it right away to keep your account safe.

If you have any questions about protecting your business's social media accounts or would like help implementing stronger safeguards, responding to an account takeover, or evaluating next steps to reduce risk and protect your brand, please contact Doug Cherry or another member of Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line.