

A yellow triangle pointing downwards, located to the left of the 'BLOGS' header.

BLOGS

Archives;Privacy & Information Security;Social Media & Technology;Workplace Policies

Two-Factor Authentication Is a Necessity for Companies

It seems as though every other week brings news of a new social media hack. Last week, Crayola had hackers post inappropriate content on its Facebook page, and the official Twitter feed of U.S. military's Central Command was briefly taken over by ISIS sympathizers. Such incidents inevitably bring with them bad publicity, as well as a panicked scramble by the hacked entity to try to regain control of its account.

The problem is that having just one layer of password protection makes an account ripe for hacking. A potential hacker can either guess or learn the answers to secret questions to reset the account's password. Alternatively, the potential hacker can launch a brute force attack in which a computer automatically runs thousands of common passwords or letter combinations through the login screen to try to discover the correct password. Some have speculated that the infamous celebrity nude photo iCloud hack from last fall was perpetrated in this manner.

One of the easiest things a company can do to reduce the risk of an embarrassing hack is to set up two-factor authentication on their social media accounts. Two-factor authentication essentially provides a double layer of password protection. It commonly involves the social media provider sending an automated text message or email with a temporary, secondary login code to a pre-set recipient when someone tries to access the users account from an unknown computer or mobile device. This way, a hacker trying to gain access to the account password will be prevented from doing so without the second code. In addition, an added benefit is that the company will be alerted to any attempt to break-in to its account and can take additional protective steps.

Setting up two-factor authentication is not hard, and set-up information is readily available online through a search of the social media providers name and the phrase two-factor authentication. With Facebook, for example, two-factor authentication can be turned on by going into Settings then Security Settings and then Login Approvals. For Twitter, its under Account Settings then Security and Privacy and then Login Verification.

A company should also keep a tight watch over which employees have access to its social media passwords while making sure that it has an access back-up plan in place if the person with the keys to the system is unavailable.