Published on *The National Law Review* https://natlawreview.com

Twitter: Little Statements with Big Consequences for Companies

Article By:

Amy D. Cubbage

Twitter is under attack. In recent months, accounts belonging to media giants CBS, BBC, and NPR have all been temporarily taken over by hackers. The Associated Press is the most recent victim. On April 23, 2013, a false statement about explosions at the White House and the President being injured sent shock waves through the Twitter-sphere. The real surprise is the effect the single tweet had in the real world: the Standard & Poor's 500 Index dropped so sharply moments after the frightening tweet that $136 billion in market value was wiped out. While the hacking of these massive media outlets make headlines, everyday businesses are not safe from the threat, either. In February of this year, a hacker changed the @BurgerKing feed to resemble that of McDonald's, putting the McDonald's logo in place of Burger King's. The hackers posted offensive claims about company employees and practices. If accounts belonging to well-established companies like these are vulnerable, so is yours. If a tweet can have a profound impact on the nation's stock market, imagine what an ill-contrived tweet could do to your business.

Business owners may have the knee-jerk reaction to delete their Twitter account, but despite the recent blemishes to its security, Twitter remains one of the most important social media sites out there. Just recently, the Securities Exchange Commission made clear that companies could use social media like Twitter when announcing key information in compliance with Regulation Fair Disclosure. Twitter is not just a marketing or PR tool—Twitter is business. And you should never turn your back on existing business. So instead of hanging up your hashtags, consider some steps that can make your Twitter account safer.

Limit Access

Not every employee should have access to the company's Twitter account. In fact, hardly anyone should, except a few designated employees like the marketing director or business owner. While those with access may never do anything harmful to the account, the more people who have the log-in information, the more likely it is to fall into the wrong hands.

Create a strong password

I know, you already have too many passwords to remember. But a creative password is your best defense against someone seeking to break into your account. Employers should, at minimum, have

unique passwords for their most commonly used media sites; please do not use the same word for your Facebook, LinkedIn, and Twitter account. Once a hacker figures it out, they have control of your *entire* social media presence.

When creating a password, avoid using anything that would be too common. “Password,” “1234,” or the business’s name should never be the only thing standing between you and a hacker. The longer the password, the better. Use a mix of uppercase and lowercase letters, numbers, and symbols.

National Law Review, Volume III, Number 127