QUICK REFERENCE

POSTING INFORMATION ON SOCIAL MEDIA

Objective

Post information on social media safely.

Social media, like Facebook and Twitter, are being used more often to communicate with clients. However, these platforms are not designed to share confidential information—they may be hacked and the information shared may be made public.

Social media is great way for companies to communicate in order to interact with online clients, send messages and develop an online brand. However, if used improperly, hackers can get access to the networks and post malicious content. The choice of the type of messages to post also allows companies to stand out from malicious sites or pages that are being used for phishing.

Target recipients: Community managers and communications employees

Last update: 2017-06

Recommendations

Only share non-confidential information on social media

- Post public information: news, product descriptions, etc.
- For contest and promotions: only first and last names, addresses (mailing and email), age and phone number in the file may be requested.
- Don't insert a link that asks clients to enter personal or confidential information (e.g., a contest) or download a file.

Make a list of your social media and online community accounts

- Determine the criteria for selecting the sites you're going to use to open a business account.
- Don't entangle your social networks (e.g., log on to Twitter using your Facebook account).

Administrator accounts should…

- Be protected with strong passwords: minimum of 10 characters. Create a password using one of these two options:
    - Option 1 : Create a password using a mix of letters and/or numbers
        - Tip: Use the first letters of each word in a sentence
        - Example: The sentence "My little dog Fido is a brown pure-bred Chihuahua"

becomes "mldfiabpbc"

- Option 2 : Create a password using at least 3 dictionary words (be careful to avoid some words).
  - Example : tablegrasswalk
  - Never create a password using words related to your personal or professional life, such as the name of your spouse, child or pet, the brand of your computer or mouse, the bulletin board thought of the day, a season, day of the week, month or year.

- Be protected with unique passwords: don't use the same password for different accounts.
- Have confidential passwords: the administrator account password must never be disclosed to anyone.

Send information from the business account

- Only give access to administrator accounts to authorized persons.
- Immediately delete administrative access when an employee leaves the company or changes jobs.
- Watch out for imposters who claim to be employees or from your company.

Run Facebook Security Checkup for all administrator accounts to…

- Log out of Facebook from unused browsers and apps.
- Get alerts when someone tries logging into your account from an unrecognized computer or mobile device.

If your account is hacked

- Immediately secure a hacked account by going to the **Facebook Help Center** > **Privacy and Safety** section, Hacked Accounts page.