REFERENCE SHEET

POSTING INFORMATION ON SOCIAL MEDIA

Purpose of the document

Post information safely on social media.

Social networks such as Facebook and Twitter are increasingly being used to communicate with clients at large. However, these platforms must not be used to discuss confidential information because they are prone to hacking, and information exchanged can be made public.

Social media are a good way for companies to communicate and interact with clients online, convey messages, and build their brand. That being said, improper use of social media can help ill-intentioned people steal access rights to the networks used and spread harmful content. Plus, by choosing the right messages to post, companies can stand out from fake sites or pages that try to phish their clients.

Recommendations

Only exchange non-confidential information via social networks

- Send public information: news, product descriptions, etc.
- For contests and promotions: only first and last name, addresses (email and postal), age, and telephone numbers on file may be asked.
- Do not insert links that would prompt clients to enter personal/confidential information or upload/download a file.

Making a list of your accounts on social media and in virtual communities

- Establish criteria for selecting sites where you want to open a company account.
- Avoid intertwining social media (e.g. logging on to Twitter with your Facebook account).

Protect administrator accounts

- Use complex passwords (at least 10 characters) in keeping with either of these two options:
    - Option 1: password containing random letters and/or numbers
        - Tip: Use the first letter of each word in a sentence
        - E.g. The sentence "My dog Fido is a white purebred poodle that barks" becomes "mdfiapptb"
    - Option 2: password made up of at least 3 words, excluding words to be avoided

        - E.g. tablesheetmountain
        - Avoid words associated with your immediate environment or personal or professional life. E.g. name of your spouse, child, pet; the brand name of your computer or mouse; a saying posted on the bulletin board; the season, day of the week, the month or year.
- Use unique passwords: Do not use the same password for different administrator accounts
- To protect your passwords: an administrator account password must never be communicated or shared.

Sending information from the company's account

- Limit access to administrator accounts solely to authorized individuals
- When an employee leaves or changes position, immediately remove their administration accesses
- Watch for imposters who pretend to be employees of your company.

Advantages of launching Facebook's Security Checkup for all administrator accounts

- Log out of Facebook on inactive applications and browsers
- Receive alerts when someone tries to log into your account from a new computer or phone

If an account is hacked

Immediately secure any administrator account that has been hacked. Simply go to the Account Security section on Facebook's online help on the Hacked accountspage.