CMSGu2015-03

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Responding to Social Media Attacks

National Computer Board
Mauritius

Version 1.0

June 2015

Issue No. 3

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to provide users of social media with the stepping stone to deal with social media attacks, whether it is for personal reasons or business purposes.

1.2 Audience

The target audience for this guideline includes all users of social media such as Facebook, Instagram, Pinterest and Twitter.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 explains how to handle personal attacks on social media

Section 3 illustrates how to respond to social media attacks on brands

Section 4 concludes the document.

Section 5 contains a list of references that have been used in this document.

2.0 Handling personal attacks on social media

Social media is a powerful tool that has many professional and personal advantages, which is one of the main reasons it is so popular over the world. However, while you do have control over how you build your online presence, you typically lack control about what others say about you in online comments.

The larger your presence, the more likely you are exposing yourself to feedback, both positive and negative. Even if you have not built out your social media presence, you run the risk of being exposed to one of social media’s dark sides: the personal attack.

2.1 Anybody can be a publisher (or an attacker)

When you are attacked on social media, it can feel like the community has already made its mind up about you until you can prove your innocence. In the past, traditional media typically filtered mass messages to particular audiences, limiting the likelihood of harm as well as its effects. Now, anyone is a publisher to unlimited, worldwide audiences, without nearly as many filters. This greatly increases the potential for harm.

In this environment of instantaneous outbursts of micro-messages, the damage is done the instant something is tweeted or posted online. What is posted online can also be reposted and continue to live long after the original message has been deleted. Those attacked now have a greater need to minimise harm to their reputation, and to do so quickly.

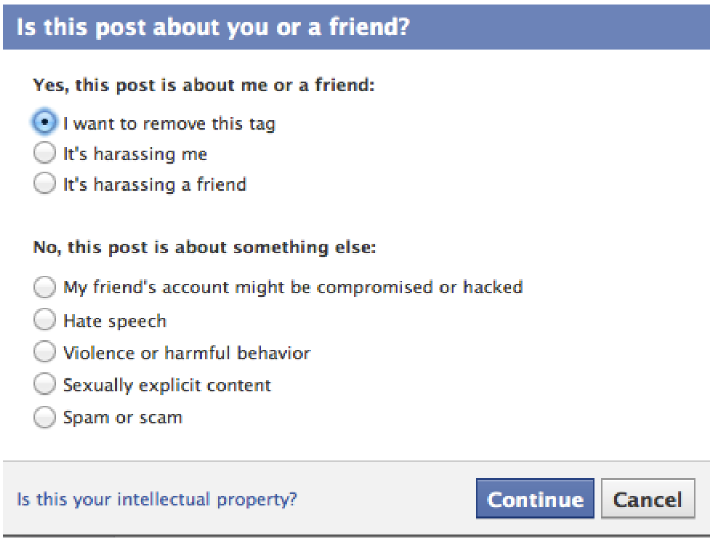
The form of the harm can be much more complicated too. People can incorrectly take a comment you make out of context, they can share hurtful opinions, expose a truth that is humiliating to you.

Social media sites have typically taken a hands-off approach to personal attacks launched by one user against another.

Twitter currently provides a form for reporting abusive users and details of the behaviour. It also suggests contacting local authorities to resolve the issues offline “if the interaction has gone beyond the point of name calling.”

Facebook also provides guidelines for reporting violations. It suggests hiding the abusive item from your news feed, sending a message to the poster asking them to take the item down, and unfriending or blocking the person.

Near every Timeline post, Facebook provides a tool that lets you report harassing or offensive behaviour:



Is this post about you or a friend?

Yes, this post is about me or a friend:

● I want to remove this tag
○ It's harassing me
○ It's harassing a friend

No, this post is about something else:

○ My friend's account might be compromised or hacked
○ Hate speech
○ Violence or harmful behavior
○ Sexually explicit content
○ Spam or scam

Is this your intellectual property?

Besides reporting an offensive tweet to the site, or reporting someone to the police if the harm is severe enough, here are few things you can do if someone says something degrading about you or your organization:

2.2 Responding to an attack

There are a number of effective strategies for overcoming the harm caused by a personal attack on social media. And your response can be a democratic one that includes fighting bad speech with more (good) speech.

1. Do not panic.

While this seems like a social media crisis, know that you are not the first person to experience the nastiness of such an attack. Do not panic. Suspend judgment. Do not take what has been said personally. Resist the urge to react right away

Instead, take a deep breath and think about what options exist.

2. Figure out if (and how) you want to respond.

Consider the motivation of the attacker:

- Are they just seeking attention?
- Are they misinformed?
- Based on this, what is the best approach?
- What value would come from engaging with the attacker?
- What is the best way to minimize any harm caused by the situation?

Insults on social media are pretty much the same as insulting phone calls, emails, letters – we have all received them at some point in time. The bottom line is the insulter is just trying to get a reaction; responding just fuels them.

- Does your organization have an existing comment policy or social-media guidelines that can guide you in this situation?
- If yes, how can you apply that policy to help you decide what next steps to take?
- If not, how can you help your organization create effective guidelines to better handle situations like this?

Be sure to save the posts by taking a screenshot or saving the post to a file. If the posts get excessive or threatening, consider letting your manager know about the abusive behavior and informing the site where the attack originated. Also consider blocking the attacker from tweeting at you or posting about you on Facebook, with the understanding that this will not keep them from posting about you to others.

3. Respond quickly publicly and then take the follow-up conversation offline

In most cases it is good to respond quickly in the same venue where the attack was made by sending a brief, temperate message recognizing you saw the attack. Then, if appropriate, try to follow up in a more private way, such as a phone call or email. Consider what value would come with taking the conversation offline. Figure out your goals for a follow-up conversation and let them drive your communication.

4. Damage control: Determine how to best remedy the harm. Can’t I sue for defamation?

In traditional media, when someone makes a false statement of fact to someone else that harmed your reputation, the typical remedy would be to sue that person for defamation or slander. Reaching a resolution often involves a defamation lawsuit that can potentially last for years.

In social media, that remedy is not as effective. A lawsuit is not quick enough to mitigate harm. Many times the harm someone causes in a comment or post online would not even fall within the purview of defamation, because it is not an actual false statement of fact. In some case, an attack can be hurtful, but not technically defamatory.

2.3 Planning in advance

While you cannot always anticipate when someone may post something hurtful or harmful, it is helpful to develop a plan in advance for how you will respond to such a post thoughtfully.
To develop your plan, ask yourself these questions:

a) How will I monitor what people are saying about me in social media and online posts so I can respond quickly?
Set up an alert using **Google**, **Talkwalker** or **Mention** so you are aware when someone says something about you or your organization. Also, frequently monitor Twitter and Facebook to see when someone has mentioned you.

b) What can I learn from teachable moments?
Outline scenarios you have seen people or organizations face and use these as teaching moments. Examine how people and organizations handle their social media attacks. What do they do that works well? What would you do differently?

Use these real-life situations that fortunately do not involve you to consider what your response would be in that situation. Or actually draft an action plan with example responses to use if you ever face a similar situation.

c) How can my social media use support a strategy?
Both organizations and individuals should have strategies that guide their social media use. Organizations should have a clear sense of their content goals, and how

social media can help them reach these goals. How you respond to an attack can be a reflection of your employer as much as it is a reflection of yourself.

It is helpful before you or your organization faces a social media crisis to have values-based conversations about common ethical pressure points you confront in social media. For example, how transparent should you be about your work in posts? How should you reflect your biases and your beliefs in your social media posts?

Social media is personal and lets you reveal as much about yourself as you decide you want to. Individuals should also take responsibility for what they post online, and create personal strategies to guide them.

A social media attack can be your opportunity to make something productive for your personal brand. When you are aware, proactive and strategic, you can not only mitigate harm from a social media attack but also use the incident to build and enhance your impact on those you reach through social media.

3.0 Responding to social media attacks on your brand

Online brand and reputation attacks have become some of the easiest and most impactful mechanisms for individuals and companies to cause serious harm to businesses.

These types of attacks can originate from a variety of sources, but most commonly the "attackers" are competitors, disgruntled employees, unhappy customers, dissatisfied investors, extortionists or other people and businesses who become upset with a company and want to cause that company serious damage.

Further, these attacks come in many forms, including:

- Posting defamatory comments on complain websites
- Posting false information on social media websites or apps, including Facebook and Twitter
- Anonymously sending defamatory emails to clients or customers
- Posting false reviews on Yelp or similar websites
- Altering Wikipedia entries about a company or particular executives in an embarrassing or otherwise harmful way
- Creating websites or blogs and posting disparaging information on these platforms

Considering the ease with which these types of attacks can be initiated, and because of how quickly content can spread on the Internet, online reputation has become a top concern for businesses and executives. A primary cause for such concern is how easily and quickly information can spread on the Internet and social media, and the resulting potential of widespread damage.

3.1 Should you respond to attacks on your brand?

If your brand or business is being harmed on the Internet, you should know what the proper response is, if there is any.

First, it is necessary to evaluate the attacker's characteristics and find out as much information as possible about the attacker and whether they pose a significant threat.

More specifically, it will be important to determine the following:

- Whether this is likely a one-time attack by a disgruntled party or the beginning of a full-fledged campaign attack;
- How sophisticated the attacker is;
- Whether the attacker has a large social media and online presence or following; and
- How likely the attacker might be to spread the information around the Internet in highly visible places.

The potential for the information to spread and be seen by large audiences, even if not highly visible today, is particularly important for several reasons. This includes statute of limitations considerations, as that begins to run the day material is first posted online. Even if the harmful content does not initially rank highly on search engines, it eventually could appear on the first page of search engine results (even after the statute of limitations has expired).

At any point in time, a person could hyperlink to the defamatory post somewhere that will reach a significantly higher number of people searching for your business. Thus, in evaluating the potential harm, your company should consider the probability that the information could spread anytime in the future and, if not dealt with, it could leave the harmed party without legal recourse.

When your brand has been attacked online, considering the factors outlined above is just a fraction of the analysis. However, there are additional issues that you need to tackle, for instance:

- What if your attacker is anonymous or used a pseudonym?
- How do you identify an unknown attacker?
- When or once the identity of an attacker is known, what are your options and which techniques are best?
- Can you recover damages?

4.0 Conclusion

Social media is an everyday tool that allows people to communicate, stay in touch, market their brands, buy and sell products and so forth. However, if used by the wrong people with bad intention, it can have a devastating effect. Consequently, it is important to know how to tackle different types of attacks in a strategic manner on social networking sites.

5.0 References

www.socialmediaexplorer.com

http://www.zillow.com

www.prnewswire.com

www.jeffbullas.com

www.wragge-law.com

http://tbwhs.com

http://agsci.psu.edu

http://mashable.com

ww.entrepreneur.com

www.poynter.com