Our Non-Profit Provides Educational Resources to Help Businesses Protect Their Brands and Reputations Online

The Online Reputation & Brand Protection Coalition’s mission is to help businesses protect their online reputations and brands online. The Coalition aims to fulfill its mission by educating businesses on how to protect and defend their reputations and brands online and advocating for increased protections and more effective remediation options for businesses.

Specifically, with respect to education, many businesses today are struggling because they do not understand how to best protect and defend themselves against online reputation and brand attacks, and there is presently a lack of quality educational materials and resources for businesses to turn to help understand and address these problems. To address the absence of these resources, the Coalition is committed to providing resources to businesses with the most up-to-date information designed to explain, prevent, and help businesses ultimately eradicate the problem of online reputation and brand attacks.

The Coalition provides its members with whitepapers created by the experts who regularly handle online reputation and brand attacks around the world addressing common reputation and brand problems which businesses are facing today.

BOARD OF DIRECTORS

Whitney C. Gibson  
Co-Founder, Co-Chair of Board of Directors  
wcgibson@vorys.com

Chris Anderson, PH.D.  
Co-Founder, Co-Chair of Board of Directors  
chris@cyberinvestigationservices.com

Melissa Agnes  
Member of Board of Directors  
www.agnesday.com

ABOUT THE ONLINE REPUTATION & BRAND PROTECTION COALITION

The Online Reputation & Brand Protection Coalition is a non-profit organization dedicated to helping businesses protect their reputations and brands online. The Coalition is led by internet brand protection experts Whitney Gibson and Chris Anderson and includes a variety of multi-national advisors comprised of experts, business representatives, attorneys, educators, and other professionals.

To learn more about the Coalition, visit www.onlineprotectioncoalition.org
Internet Harassment and Stalking
Online: Best Practices

I. Introduction

In fact, there are many “adult” harassment campaigns launched for the purpose of alarming, scaring, or harming the reputations of others.

There is a common misconception that online bullying is only an issue with young kids and teens. However, there are hundreds of cases being reported to law enforcement officers each week by adults that have been on the wrong side of these attacks. In fact, there are many “adult” harassment campaigns launched for the purpose of alarming, scaring, or harming the reputations of others. Similar harm can be caused through online stalking as well.

It is important to note that there is a difference between “cyber” stalking and harassment (although the lines are often blurred). For example, according to Florida’s criminal statutes—similar to those in many other states—both cyberstalking and cyberharassment involve engaging in conduct directed at a specific person that causes “substantial emotional distress to that person and serves no legitimate purposes.”

While cyberstalking and cyberharassment are distinguishable, this whitepaper provides an overview of steps that should be taken when faced with both types of “cyber” attack.
II. Defining Cyberstalking, Cyberharassment

According to the National Conference of State Legislatures (NCSL), cyberstalking is defined as “the use of the Internet, email, or other electronic communications to stalk, and generally refers to a pattern of threatening or malicious behaviors. Cyberstalking is further characterized by there being “credible threat of harm.”

Cyberharassment, however, typically does not involve such a credible threat and it may (although not always) also involve electronic communications of words or images. According to the NCSL: “Cyberharassment usually pertains to threatening or harassing email messages, instant messages, or to blog entries or websites dedicated solely to tormenting an individual.”

Most often, we see cyberstalking and/or cyberharassment occur from or through the following methods:

- Email, instant messaging, or SMS and MMS messaging;
- Voice over IP (VoIP) calls, such as via Skype;
- Fake social media accounts;
- Posting photographs or statements on online forums (such as on Instagram);
- Hacking into computers or other electronic devices, including into specific accounts;
- Spyware; and
- Intercepting communications

Of course, cyberstalkers and cyber harassers can use these means and other tracking of the locations of victims to physically stalk or cause other harm to these people.
III. Dealing with Cyberstalking, Cyberharassment

If you are being stalked or harassed online, remember the following:

1. **Don’t Panic** – These types of cases can usually be solved by utilizing technical and forensic investigations, combined with legal action.

2. **Report these cases early** – Most people wait too long to report or take action, which causes paranoia (or the aforementioned panic) in the victim and empowers the suspect. Report it to the police and get a case number. They are required by law to take a report. If law enforcement will not intervene, you should seek the help of private investigation firms that handle stalking and harassment matters.

3. **Understand many of these cases involve someone you already know** – While there are “unknown stalkers,” most of the time you know them. Also understand that most stalking cases that carry on for more than a week or two typically involve someone with a psychopathic or sociopathic personality (and those continuing beyond a few weeks is likely to continue indefinitely without intervention).

4. **Document everything** – Document every communication you receive; it may become important evidence later. Moreover, a skilled investigator can isolate a case to certain types of technology and skill being used by the attacker, and track down the stalker based on forensic evidence. Thus, keep track of what device you received the threat from, the time of day, who was around you, what room you were in, who witnessed it, and similar details. For example, it is typically possible to screenshot a phone screen and save the image when dealing with text messages. This is important for sorting out the technological methods being used by the attacker for intercepting and delivering communications.

5. **Understand that most police departments do not have the training or staff to investigate these types of cases** – While this is frustrating for most people, the truth is that technology and the volume of these types of cases have outstripped the police’s capabilities of handling these types of crimes. Once evidence can be provided by a professional third party, the police often will then take the case. However this will vary from jurisdiction to jurisdiction. Also, realize that many police departments do not know what jurisdiction your stalker is in and, therefore, will refuse the case based upon that. However, once jurisdiction can be established, then the police department that you are dealing with should be in the jurisdiction of the attacker.

6. **Seek assistance from cyber professionals** – Seek a professional cyber and forensic expert that has experience in investigating these types of cases. Due to the variety of attack methods, this requires a professional who is familiar with all of the technology and how to obtain the necessary evidence.
IV. Conclusion

It is very difficult for a serial harasser or stalker not to make critical mistakes in the process of carrying out his or her campaign.

Being harassed or stalked online is obviously not desirable, but if you end up as the victim of such behavior, remember that you are not helpless. With cooperation between a good cyber investigator and a legal team, the odds of catching cyberstalkers and cyberstalkers are 95 percent or greater. It is very difficult for a serial harasser or stalker not to make critical mistakes in the process of carrying out his or her campaign. In order to do this, you must first get the technical evidence needed that will stand up in a court of law. A skilled cyber and forensic investigator can assist with this. Once such help is obtained, a qualified attorney can help you file the legal case, get restraining orders against your attackers, and potentially collect damages from your stalker or harasser.