crash override

online abuse helpline & resource center

## What is online abuse?

Online abuse can encompass a wide variety of things, but often manifests as sending someone hateful messages online, campaigns of character assassination, hacking, stalking, threats, and a number of other things. Unfortunately this often escalates into targeting the victim's friends, families, and employers in an effort to isolate the original target and cause as much damage to them as possible.

## Why is this happening?

People can become targets of online abuse for any number of reasons, ranging from a continuation of offline abuse, their identity (race, gender, sexuality, etc), or even a case of mistaken identity. It's important to know that this can happen to anyone for any reason at all, and does not automatically indicate any sort of misbehavior by the employee.

## What should employers expect?

One common way that attackers typically harass people is by bombarding a target's place of work with messages, false complaints, and threats in a coordinated attempt to get them fired. Threats can range from physical (such as calling in security emergencies) to commercial (threatening to cancel pre-orders, return a product, or spread slander about the company). This is meant to pressure the employer into feeling that the employee is too much of a risk to their business and either terminate their employment or force them into silence, even if the threats are empty and complaints without merit. Oftentimes, attackers will do this by inflating their numbers (by recruiting more people or creating many fake accounts), or other hoaxing tactics to make themselves seem like a more significant threat to the company, and to make online harassment falsely appear like legitimate public outcry. These campaigns can widely vary in terms of scale and duration, but are commonly quite brief if the company is unresponsive.

## What can employers do?

First and foremost, employers should take great care to not give out any personal information pertaining to their employees without asking their employees for their consent first. It's not uncommon for attackers to try to tease out more information on their targets in this way, and employers should not allow themselves to be used to violate their employees' privacy.

We strongly encourage employers to try to understand the situation their employee is in when they are targeted by online abuse, and work with them rather than punish, terminate, or silence their online activity outright. This can be especially damaging for employees working in creative or technological fields, where their livelihood may be reliant on or enhanced by maintaining their online presence. Attacks of this nature are often highly personal, complex, and difficult to understand or evaluate at first glance. It is important for employers to investigate the merit of the claims or threats before acting, and to discuss them with the employee for further context and clarification. This allows for more informed decision-making, rather than a kneejerk reaction to online misinformation and social engineering. A company's capitulation to empty threats or baseless accusations from an attacker often encourages them to continue these tactics should they ever wish to get the employer to hurt someone else on their behalf.

Once an informed decision is made, employers should use caution when engaging with the attackers, if they engage at all. Not only are bad faith threats of boycotting and backlash often empty, a company's capitulation to falsely manufactured pressure, if publicized, can be disastrous. The public perception that a company has responded inappropriately to hoaxes or abuse is often far more damaging than any small-scale, fleeting positive attention a company may receive from the instigators of a campaign of abuse. Respectable and influential publications and news outlets will rarely investigate and follow up on unfounded or transparently meritless outrage at a company from online harassers, but are quicker to report on a company inadvertently siding with someone's attackers out of fear or risk-aversion.

For example, during one such controversy, Intel quickly bowed to pressure from a small group of abusive people registering hundreds of accounts, demanding that they remove their advertisements from a website that several of their targets worked at. After later realizing their mistake due to the resulting media fallout, Intel not only reinstated their advertisements, but apologized and pledged $300 million to support inclusivity initiatives in tech. This kind of confusion and reversal is sadly common in cases of workplaces being targeted, and can be devastating for all parties.

This is only meant to be a brief fact sheet - if you have any further questions about the nature of these situations and best practices, please feel free to contact us at help@crashoverridenetwork.com, where we can offer pro-bono advice and resources for people affected by online abuse, including information security audits, monitoring services, and general information.

## For More Information, Go to CrashOverrideNetwork..com