CREATIVE EQUALS

stopit

Dealing with Hate Hacks:

A Policy Document Introducing the STOPIT Protocol

Lydia Amoah

To find out more contact:
hello@creativeequals.org or visit creativeequals.org

INTRODUCTION

In March 2020, the UK government initiated an unprecedented lockdown in response to the declaration of a global pandemic by the World Health Organisation. The actions of the UK government turbocharged a trend already long in the making, i.e., the rise of home working and the mass digitalisation of activities associated with gainful employment. In a seemingly effortless manner, millions of workers have taken advantage of information and communication technologies and transitioned from physical office spaces to the use of online digital interfaces.

As would be expected, entry into this new working environment has involved the discovery of novel challenges, hazards and harms, some of which involve serious crimes. The rapid pace of change has placed industry, government, and third sector organisations on the back foot in addressing cyber-harms. This document addresses a novel but highly prevalent cyber-harm: hate hacking. It defines the issue and provides a person-centred protocol for dealing with the occurrence of hate-hacking.

The genesis of the current document lies in a real-life, pernicious attack upon the chief creator of this policy. Lydia Amoah, whilst delivering a public webinar on the Zoom platform, was subject to a hate hack. A group of international hackers gained access to the meeting and proceeded to share highly disturbing images. They then singled out Lydia and subject her to appalling verbal, racially-motivated abuse. This occurred in front of an online audience of 100+ industry peers.

CREATIVE EQUALS stopit

OUR VISION

Employers have a legal and ethical obligation to ensure the physical and mental safety of employees and other associated stakeholders. Our vision is to help companies meet and fulfil the duty of care which arises from the need to ensure employee safety in the online working environment. According to the UK government white paper 'Online Harms' (2016), businesses have a duty of care to ensure that appropriate safety systems and processes are put in in place when operating in the online environment.[1]

In this document, we specifically address the abhorrent practice of hate hacking and the need to implement an incident management policy and process. In doing so, we put forward a simple robust, and effective protocol which places the needs of the target of the hate hack at the centre of all aftercare activity. The STOPIT protocol details the step-by-step actions which should be taken following the occurrence of a hate hack.

Embracing the STOPIT protocol and guaranteeing its implementation in the case of a hate hack will ensure that employees and other stakeholders feel safe whilst using digital interfaces for work-related purposes. It will also ensure that employers feel equipped to manage the immediate situation as well as mitigate the harm which arises from the occurrence of a hate hack.

[1] https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper

CREATIVE EQUALS stopit

THE IMPACT OF HATE HACKING

Agrafiotis et al. (2018) detail the impact of cyber-harm on individuals and organisations.

The psychological impact activities like hate hacks have on targeted individuals include symptoms such as depression, embarrassment, anxiety, and reduced confidence.Amongst other parties (including other employees, stakeholders, management) psychological symptoms often accrete around a perceived lack of preparedness, which can include symptoms such as projected shame (onto the organisation), resentment towards the organisation, and reduced trust.[2]

Agrafiotis et al. (2018) also discuss wider impacts of cyber-harm on organisations which can include staff retention issues (for example, key staff leaving), damage to the company brand, and even critical media scrutiny.

[2]Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D., (2018). Taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity 4 (1), 1-15.

[3] https://www.cps.gov.uk/hate-crime

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/839172/hate-crime-1819-hosb2419.pdf

[5] https://www.cps.gov.uk/cyber-online-crime

WHAT IS THE PROBLEM

Very simply, there is an acute lack of preparedness in relation to dealing with the cyber-harm that arises from hate hacking.

What is hate hacking?

According to the U.K. Crown Prosecution Service (CPS):

'The term 'hate crime' can be used to describe a range of criminal behaviour where the perpetrator is motivated by hostility or demonstrates hostility towards the victim's disability, race, religion, sexual orientation or transgender identity'.[3]

In the reporting year of 2018-19, the police authorities of England and Wales reported the highest ever number of hate crimes on record: 103,379 in total – a year-on-year increase of 10 per cent and more than double the 2012-13 figure.[4]

The CPS define 'hacking' as:

'. . . the unauthorised use of or access into computers or networks by using security vulnerabilities or bypassing usual security steps to gain access'.[5]

Bringing together the concepts of 'hate crime' and 'hacking', we define 'hate hacking' as activity which involves intrusion to digital interfaces and assets by unauthorised, threatening individuals who act with an intent to abuse or cause distress to the target on grounds of invidious prejudice (i.e., race, ethnicity, religious belief, sexual orientation, disability, and gender identity).

We should note that general abuse of someone online can be construed as a criminal offence. The Communications Act 2003 details that using electronic communications to send grossly offensive, indecent, obscene, or menacing content is a crime. And so, we also recognise a wider sense of the concept of 'hate hacking' in which similar activity described above is perpetrated with the intent to abuse or cause distress to innocent individuals but not necessarily on the grounds of invidious prejudice (i.e. generalised abuse). A pertinent example of this is provided by the online hate hub (funded by the London Mayor's office in 2018) which tracked abuse against several groups,[6] including those who receive online abuse but do often do not fall into one of the protected hate crime categories, such as Goths.

Are organisations prepared?

The Cyber Security Breaches Survey (2019) reported that only 36% of companies surveyed had cyber-security contingency plans in place (most of which seem to involve software measures like firewall protections not aftercare processes).[7] Just under three in ten businesses (27%) reported that staff had attended internal or external training on cyber-security. More worryingly, just 16% of companies reported having incident management plans.[8]

Agrafiotis et al. (2018) note that recent changes to the legislative environment (namely the European General Data Protection Regulation, 2016) which makes more stringent requirements of companies may be leading to a situation whereby companies are wilfully blind to the issue of cyber security. As a societal trend, this may be leading to a business culture of 'organised irresponsibility' (Agrafiotis, 2018: 3).

[6] https://www.bbc.co.uk/news/uk-england-london-39692811

[7] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

[8] Ibid.

THE STOP IT PROTOCOL

The online world is a dynamic, ever-changing landscape where novel threats frequently emerge. Although the specific details of a hate hack occurrence may differ, the person-centred nature of the STOPIT protocol should enable responsible individuals within an organisation to navigate a hate hack.

Furthermore, if an individual outside of your organisation is the target of a hate hack during an event for which you are responsible, we suggest every effort be made to reach out to the individual and offering as much support as possible.

Before embarking on any online activity, ensure you follow online security measures (see Appendix 1) for a provisional list of security measures). If possible, it is advisable to involve or consult an individual with relevant expertise in information and communications technology.

CREATIVE EQUALS
stopit

Stop all activity.

The current activity should be immediately brought to an end.

STREAM 1: DEALING WITH INTERNAL MEMBERS OF STAFF/DIRECT TARGETS OF THE HATE HACK

Targeted individuals must take priority.

If a specific individual or group of individuals have been targeted then there should be an immediate provision of a safe space in which the individual/s can be listened to and offered comfort. Ask if there are any remedies at hand which the target/s of the hate hack would like to have (for example, working offline for the rest of the day, or taking time off work).

Offer further in-depth-support to targeted individuals.

Direct the target of the hate hack to further pastoral support services (e.g., NABS Counselling, Victim Support, Samaritans, The Monitoring Group, Gallop).

Prepare to report the incident.

The 'Online Harms' (2016) white paper calls on companies to develop effective reporting mechanisms for cyber-harm. If your company does not have an HR department, it is advisable to appoint a person responsible for recording cyber-harms. Capturing the hate hack event in as much detail as possible can allow for reporting to the online platform and the police.

In terms of reporting to the police, several options exist for reporting hate hacking incidents: calling 999 emergency line; attending the local police station; or, for those wishing to remain anonymous, calling Crimestoppers by phoning 0800 555111 or by visiting www.crimestoppers-uk.org and completing the online form.

IT Security check.

Conduct a diagnostic security check so as to check all feasible security measures were/are in place. You may wish to refer to the checklist in Appendix 1.

Team check-in.

At an appropriate time, gather with the members of staff present to discuss and reflect on the incident. Attendees can also be directed to further pastoral support services if necessary.

Depending on the wishes of the individual targeted, it may be appropriate to share the experience of the incident (of course respecting the anonymity of the individual and those present). Recommended platforms for advocacy are Victim Support, Samaritans, The Monitoring Group, Gallop, TellMAMA).

THE STOP IT PROTOCOL

STREAM 1: DEALING WITH INTERNAL MEMBERS OF STAFF/DIRECT TARGETS OF THE HATE HACK

1	Communicate with the stakeholder/s	Send a pre-prepared email informing the audience that due to the hate hack the meeting will be postponed to be rescheduled at a later date.
2	Offer direction to further support	Communicate further with the external audience, offering guidance on obtaining further support where necessary. Depending on resources, communication can be both off-line and/or online (e.g. email).
3	Reach out	Let the external audience know that you are logging the incident and would appreciate any thoughts or feelings they may have as a result of witnessing the incident.

THIS POLICY SHOULD BE REVIEWED ANNUALLY (7 MAY 2021)

SUPPORT NETWORKS

NABS
Colour of Change
Victim Support
Race in The Workplace
The Monitoring Group
Show Racism The Red Card
True Vision
TellMAMA
Stop Hate

Appendix 1

Below is a security checklist to use when planning and conducting an event on a digital interface like Zoom.

✔ How the event was created and promoted

(Open links shared on social media platforms can invite cyber threats into a business)

✔ Ensure someone is appointed who has tech support experience to be present at all times

✔ Appointed a second host to manage the second and third party stakeholders

✔ Send specific sign up instructions before the event

✔ Use access passwords

✔ Use waiting rooms so as to allow for vetting of those entering

✔ Manage control functions; i.e Mute/Screen sharing permissions

Acknowledgements:

I thank Dr Jamie McKeown and Ali Hanan for their contributions to the development of this policy.

CREATIVE EQUALS
stopit

CREATIVE EQUALS

stopit

To find out more contact:
hello@creativeequals.org or visit creativeequals.org