CYBER SAFETY AT WORK

10 NOVEMBER 2020

NATIONAL PERSONAL SAFETY DAY

suzy lamplugh trust

LIVE LIFE SAFE

#CyberSafeatWork

EXECUTIVE SUMMARY

Since Covid-19, there has been a major increase in the number of online platforms being used as people isolate and work from home. **Approximately half the UK working population were by definition lone workers at home** after 23rd March 2020[1].

Concerningly, a pilot study conducted by Suzy Lamplugh Trust has found that this has prompted an escalation of online abuse. Key findings highlighted that a startling **one third of participants are currently experiencing online abuse at work. Of these victims, 83% state that the abuse has escalated over the period of the pandemic**. Furthermore, the study finds major gaps in employers' provision of personal safety support for lone workers while online.

The findings set out in this report demonstrate the clear escalation of online harms and the increasingly blurred lines between work and home life as a result of the pandemic. The report highlights guidance for employers and employees to improve their safety online, as well outlining what actions platforms can take to better protect users.

> *"It has been horrible stuck in four walls with this horrible abuse"*

INTRODUCTION

According to a survey carried out by the Office for National Statistics (ONS), in April 2020, 46.6% of people in employment did some work at home[2]. Of these, 86% did so as a result of Covid-19. According to the Health & Safety Executive (HSE), lone workers are those who work by themselves without close or direct supervision[3]. Approximately half the UK working population were by definition therefore lone workers at home from the start of the pandemic.

Suzy Lamplugh Trust launched a pilot study in October 2020, surveying a total of 648 respondents, in order to ascertain the impact and experience of online abuse on lone workers at home.

> *"Upsetting and hard to deal with"*

WHAT IS ONLINE ABUSE?

Everyone has the right to online safety and privacy. Online abuse is any form of persistent and/or unwanted contact from another person that is perpetrated across social media and communication platforms. Victims come from all backgrounds and are not confined to public figures. They can do any job, be of any age, gender, sexual orientation, social or ethnic background, and live anywhere.

Online abuse can take many forms including bullying, sexual harassment, message bombing, hacking, trolling, phishing, doxxing, and digitally-enabled stalking to name a few.

> *"Just don't feel valued anymore"*

35% OF RESPONDENTS ARE CURRENTLY EXPERIENCING ONLINE ABUSE AT WORK

[1] Coronavirus and Lone Working in the UK: April 2020; 8th July 2020. https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/coronavirusandhomeworkingintheuk/april2020

[2] Ibid

[3] Health and Safety Executive, Lone Workers; https://www.hse.gov.uk/toolbox/workers/lone.htm

KEY FINDINGS

Increase in Online Abuse

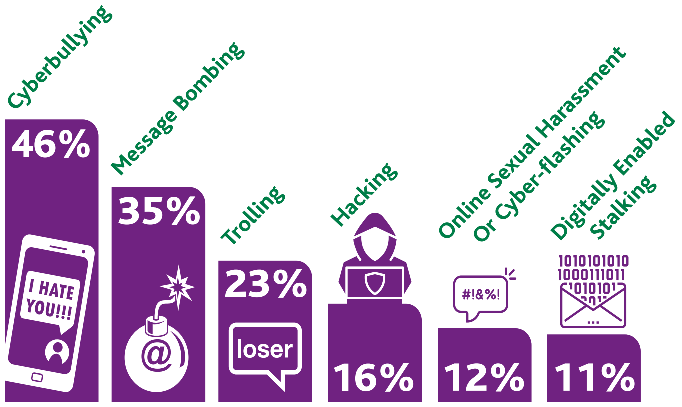
One third of all survey respondents reported experiencing online abuse at work. Of these, as many as 83% stated that over the period of the pandemic, there had been an escalation of online abuse.

Perpetrators include: colleague (29%), ex-colleague (29%), patient/client/customer (11%). **Notably, over a quarter of perpetrators of online abuse at work were either the victim's manager or superior.**

Forms of Online Abuse

A fifth of all respondents stated they have experienced cyberbullying at work.
The most common forms of abuse experienced by victims were as follows:

- **Cyberbullying 46%** (Using intimidating communication, threatening language, online threats, hate speech);
- **Message Bombing 35%** (Flooding phone, email and/or other online accounts with messages, especially out of working hours);
- **Trolling 23%** (Intentionally posting upsetting / insulting / digressive comments directed at victim on internet communities);
- **Hacking 16%** (gaining access into any online service via computer or phone);
- **Online Sexual harassment or Cyber-Flashing 12%** (Sexual bullying, online sexual comments, 'jokes' of sexual nature, gossip / lies of sexual nature, body shaming);
- **Digitally-Enabled Stalking 11%** (using any form of technology to carry out fixated, obsessive behaviour towards a victim).

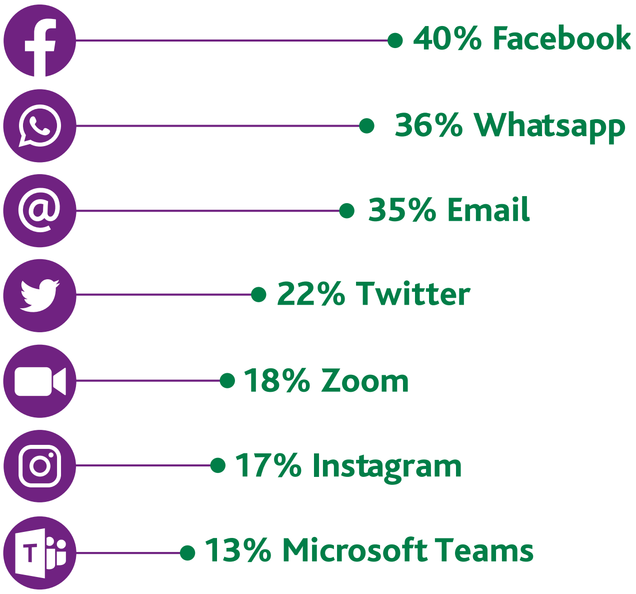


Participants also highlighted experiencing behaviours such as "Undermining during meetings, talking over etc", "Gaslighting, denial of bad behaviour when called on it", "Authoritarian, intimidating, different tone talking than in writing", "Being undermined, ostracised, intimidating behaviour, belittled, humiliated".

Three quarters of respondents felt that the abuse was targeted on their personal characteristics: 36% felt they were singled out based on their gender, 33% based on their race and 33% on their age.

Platforms Misused for Online Abuse

The three platforms through which online abuse was overwhelmingly perpetrated were Facebook, WhatsApp and Email.



Impact

Online abuse can have detrimental effects on the victim. Among the victims of online abuse within our pilot study, **92% reported that this impacted their mental health**. Of these, 39% stated that it affected them a great deal. Participants reported the following: "scared to talk online", "decreased my confidence in my work capabilities", "crying and emotionally feeling alone", "sleepless nights and can't stop thinking about it", "contributed to a mental health breakdown with stress anxiety and depression".

Dr Emma Short, Associate Professor in Psychology at DeMontfort University, has been researching the nature and impact of online abuse for 15 years. She states that: "It's been established that harm arising from online or abusive communications can be overwhelming, including significant emotional distress, feelings of isolation, anxiety and depression, sometimes initiating physiological harms such as self-harm or suicide. At the current time if people are restricted to working through digital channels which have become hostile, the sense of 'no escape' is amplified. The impact of online harm can go beyond the individuals who directly experience them, creating wider harms in the workplace where other individuals who are witness to intimidating behaviour are silenced and the usual support networks break down."

Gaps in workplace safety provision

It is vital with a second lockdown in place, that individuals working from home feel protected by their employers and the online platforms they use, in order to continue working safely online.

To explore this, participants were asked whether they received any support at work around personal safety and lone working policies. Concerningly, **over half of all respondents stated they had received no guidance in this area.** Only 19% stated that they had been risk assessed, 13% had received training, 13% knew their company policy/guidance, and as little as 5% had access to lone working apps or devices.

Half the respondents confirmed that they would like further support around their personal safety online at work.

ONLY 19% STATED THAT THEY HAD BEEN RISK ASSESSED

GUIDELINES FOR CYBER SAFETY AT WORK

The Employer: Suzy's Charter For Workplace Safety

The HSE states that employers must provide supervision, education and training, as well as implementing enough control measures to protect home/lone workers. Workers' online personal safety is paramount, especially since Covid-19 where most are working from home.

Suzy's Charter for Workplace Safety provides a personal safety framework that can help organisations become fully compliant with personal safety policies and protocols. The framework creates structures needed to ensure both employer and employee fulfil their responsibilities, including risk assessments, safety procedures and reporting.

Guidance to Stay Safe at Work according to Suzy's Charter:

1. Embed a workplace personal safety culture
2. Implement robust risk assessments
3. Provide robust reporting procedures
4. Provide personal safety training
5. Implement a tracing system
6. Have a system in place to covertly raise the alarm
7. Offer staff a personal safety alarm if necessary
8. Regularly consult on and review safety policies and procedures with employees

For further information on how to become compliant around personal safety according to Suzy's Charter, follow this link: Suzy's Charter for Workplace Safety or contact info@suzylamplugh.org

The Employee:
Advice To Be Cyber Safe At Work

Believe in your instincts. If something makes you feel uncomfortable, take a moment to explore any potential risks to your personal safety.

Engage with the online safety policy of your employer if they have one. It is your right to request changes to this if deemed necessary (e.g. if out of date). You can also request a risk assessment, education and training, supervision and support with personal safety incidents.

Check your online privacy settings. Don't share your passwords with anyone. Turn on two-factor authentication and change passwords regularly. Make sure all your social media accounts are set to private. Try Googling yourself and see if your address (e.g. 192.com), phone number or places where you regularly spend time are publicly available. There is further advice at Get Safe Online.

Your personal information (such as address, telephone number, daily routines or personal online accounts) **should not be shared with anyone online** unless completely necessary, e.g. HR might hold your emergency contact details, but these should remain confidential.

Behaviours should be documented. Keep a copy of all instances of online abuse. Devices and applications are likely to hold evidence. Moreover, social media, email, telecommunications providers and all online account providers store data on activity, log-ins and end user identifiers (such as IP address). If you use iCloud, Google, another cloud storage provider or an external hard drive these could also all be good places to search for evidence. This will be useful if the behaviour escalates or if the perpetrator deletes their posts and profiles. It can also be requested by the police as part of a live investigation.

Ensure anti-virus and anti-spyware software is installed. Make sure it is up to date.

REPORT THE INCIDENT:

- **To the police.** Report the abuse early either directly or through a report service such as www.report-it.org.uk. If you feel there is an immediate threat to your personal safety dial 999. Get further advice by contacting the National Stalking Helpline.
- **To the platform through which the behaviour is being perpetrated.** All platforms should have procedures in place for this. If you do not get an adequate response from the platform report it to Report Harmful Content
- **To your employer** (if appropriate). Check the personal safety policy at your place of work and follow the incident reporting procedure. If your employer does not have one, request it.

> *"People are more stressed and shorter tempered"*

If **Someone has hacked your computer**, or has access to what you are doing on your computer, report it to your manager or IT support through a different account for advice. For further advice contact The Cyber Helpline.

Avoid leaving your devices unprotected. Controlling physical access to your devices is key. When in the workplace, ensure your computer screen is locked, phone is PIN protected and ID documents are not accessible.

The Fault is not yours. Perpetrators of online abuse at work can be people you know (such as colleagues or managers) or strangers (customers/patients/service users). Speak to someone close to you about the abuse and contact a specialist victim support charity if you want expert advice.

Emotional responses are normal. It is common to feel your mental health has been affected by this behaviour. If you need emotional support, do not hesitate to contact your GP or Mind.

> *"As life has moved online, it feels far more invasive than previously."*

83% OF THE VICTIMS OF CYBER ABUSE AT WORK STATE THAT THE ABUSE HAS ESCALATED OVER THE PERIOD OF THE PANDEMIC

The Platform: What Is Their Role?

Our interaction with the world of technology is everchanging and in order to protect their users it is imperative that online communications and social media platforms do their best to evolve as emerging problems arise. Covid-19 has forced a worldwide transferal to online lone working and our platforms have a clear role in supporting them to be safe.

Suzy Lamplugh Trust proposes the following recommendations:

Safety Guidelines: Platforms should practise a zero-tolerance approach towards all forms of online abuse. Safety guidelines should be clear, accessible and outline unacceptable harmful behaviours. Any behaviour that fails to adhere to the safety guidelines should be addressed directly and measures should be taken to prevent further instances of abuse.

Robust transparent reporting: Suzy Lamplugh Trust calls for all social media and online communication platforms to provide the user with a robust and transparent reporting procedure. Users should be encouraged to report incidents and concerns. Monitoring of reporting times, responses to incidents and common patterns of abusive behaviour should be collated and used for improvement.

Safeguarding: We would further recommend that the platform regulators are trained in safeguarding and referring cases to specialist services. They should address incidents of discrimination based on personal characteristics, such as gender, race, age, and sexuality. The regulators should be trained to deal specifically with calls which relate to complaints involving personal safety including harassment, stalking, cyber bullying and other forms of abuse.

Ongoing Partnerships: Platforms should develop ongoing partnerships with independent specialised services that address specific types of abuse, as well as statutory services such as the police. This would enable the platform to report, share concerns and get advice if it is known that someone is perpetrating abuse on their sites.

> *"Colleagues are more fraught. Customers are more demanding and intense"*

CONCLUSION

Cyber safety at work is an issue that should be taken seriously, and the clear escalation of online abuse at work is of grave concern. With a drastic shift in our working lives, better guidelines and restrictions need to be implemented in order to best safeguard our privacy and safety. Online abuse is not part of the job. If you are a lone worker, it is important that both you and your employer give particular consideration to your safety. **Employers, employees and online social media and communication platforms all share responsibility for the cyber safety of the worker**.

> *"I feel unhappy when I have to go into work"*

A FIFTH OF ALL RESPONDENTS STATED THEY HAVE

EXPERIENCED CYBERBULLYING AT WORK

ANNEX A: ABOUT

Suzy Lamplugh Trust was founded by Diana and Paul Lamplugh following the disappearance of their daughter Suzy, a young estate agent, in 1986. Since then, the Trust has pioneered personal safety as a life skill and a public policy priority. Our vision is a society in which people are safer – and feel safer – from violence and aggression; we want people to be able to live life to the full. Our mission is to reduce the risk of violence and aggression through campaigning, education and support.

ANNEX B: METHODOLOGY

Suzy Lamplugh Trust surveyed a total of 648 respondents in October 2020. The survey was aimed at anyone who currently works in the UK, and all participants were informed that their responses would be anonymised. Those who agreed to leave a form of contact were assured that their details would remain confidential.

Out of these, two thirds were between the ages of 25 and 44. 36% identified as Cis Male, 54% Cis Female, 1% Trans Male, 1% Trans Female & 3% Other. 83% of the participants stated that their sexual orientation was Heterosexual, 6% Bisexual and 5% Homosexual. 76% of the respondents identified their ethnicity as White British, 2.3% Indian, 6% Other White Background, 2% African & Caribbean, 2% Chinese. The participants worked in a variety of industries, notably 12% in Tech & It, 11% in Education, 9% in Retail,7% in Business and Finance, 7% in Government & Public Administration, 6% in Healthcare.

ANNEX C: FURTHER FINDINGS (TYPES OF ABUSE)

Following a survey of 648 respondents, a shocking 39% of participants stated that they are currently experiencing some form of abuse at work (on or offline). **Of these, 43%** are victims of **Emotional & Psychological Abuse**, such as undermining self-esteem, name-calling, threats, coercive behaviour, gaslighting, and a disrespect of separation between work and home life. As many as **18% are experiencing stalking at work**. Of these, **11% have experienced Organisational or Institutional Abuse**, such as authoritarian management, bullying, failure to respond to abuse appropriately, and intimidating language at work. A further **9% have experienced Discriminatory Abuse**.

Note: We have used the terms 'cyber' and 'online' interchangeably in this report to include all forms of social media and communication platforms as well as technology that can be used on devices to perpetrate harmful non-physical behaviours.

LIVE LIFE SAFE
suzy lamplugh trust

@live_life_safe

www.facebook.com/suzylamplughtrust

NATIONAL STALKING HELPLINE

0808 802 0300

@TalkingStalking

www.facebook.com/stalkinghelpline

The National Stalking Helpline is run by Suzy Lamplugh Trust.
Calls to the helpline are confidential and free from most telephone networks.

Suzy Lamplugh Trust, The Foundry, 17 Oval Way, London SE11 5RR
For more information call 020 7091 0014 or email info@suzylamplugh.org