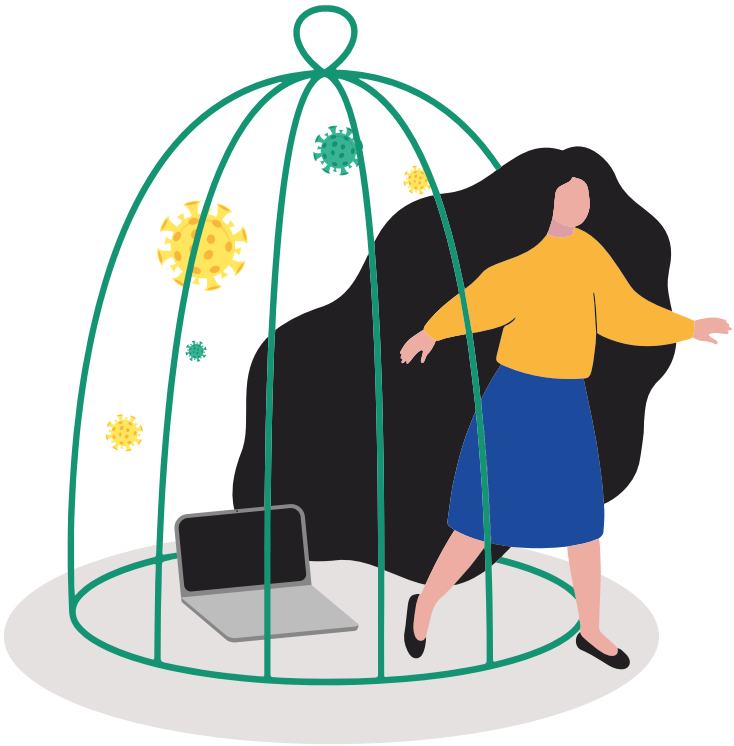
Five important tips on staying safe online during the Covid-19 Pandemic

GLITCH
End online abuse

About Glitch

Glitch is a UK based charity recognised internationally for working to make the online space safe for all by raising awareness of online abuse and its impact through an intersectional lens. Glitch campaigns for long term and systematic change from tech companies and governments and champions digital citizenship through the delivery of a range of resources and workshops on digital citizenship, digital self care and safety.



This Resource

Since the Covid-19 pandemic, living rooms, kitchen tables and gardens have turned into improvised workplaces and volunteering centres. Worldwide increases in internet usage means an increased risk to a range of online harms. This free resource provides our top key tips and advice on online safety, particularly for those working and, or volunteering from home; it can be shared with your employees, colleagues or friends who are working or volunteering from home. As a charity determined to make online spaces safer, we offer a range of training programmes on digital self care and digital self defence. We highly recommend our specialised training for employers that go further than just this resource.

If you want to equip your employees with the skills and knowledge that they need to protect themselves whilst working remotely, then find out more here:

fixtheglitch.org/bespoke-training

Soft copy can be found on our website fixtheglitch.org

Five important tips on staying safe online during the Covid-19 Pandemic

GLITCH
End online abuse

Our Covid-19 report shows that 46% of respondents reported experiencing online abuse since the beginning of COVID-19; this figure increases to 50% for Black and minoritised people. Only 9% of respondents received updated training from their employer on how to stay safe online while working from home despite the vast majority (64%) feeling that appropriate training would have been useful.

1

Digital Self Defence: Regularly install security updates on all your devices including phones, laptops and tablets and any apps that may be used for work. Doing this enables you to have the latest security fixes and helps to defend you from new online harms. We recommend setting a bi-monthly "self defence reminder" to ensure that you regularly update passwords and have two factor authentication across all of your accounts. We would also recommend that this includes a scan and review your digital footprint frequently.

2

Review your online accounts: If you see news about a data breach in relation to a company you have an account with, update your account details and change your passwords. Routinely check haveibeenpwned.com to see whether your passwords or account details have been compromised.

3

Communicate your online boundaries by having a page policy, pinned tweet, email signature or short post, which lists what you expect from others online. This is a great way to ensure your own digital self care. It can include how you plan to respond to profanity, aggressive comments, misogyny, racism, sexism, ableism, homophobia and transphobia. It can also explain how you will engage with trolls and topics that aren't up for debate; it may give an explanation of the best avenues to contact you through, or expected response rates. Through explaining these boundaries, you may feel like you're no longer having to continuously explain yourself, or communicate with those who overstep these boundaries.

4

Educate and inform employees about online abuse, digital safety, digital self care, online gender-based violence and related topics. We recommend reading Crash Override Network's useful one-pager explaining what employers can do in cases of online abuse against their employees.

Creating online resources, new policies on online conduct and allocating funding to support additional learning, and develop prevention strategies that could be deployed to better equip individuals with the tools needed to respond to online abuse in the most effective, supportive manner possible.

Form a committee to investigate complaints filed by women and those from marginalised communities in the organisation which includes racist, sexist and gender based online abuse within the organisation. Ensure that this committee consists of at least one person of colour and/or one person from the LBT community.

5

Call on your employer to offer training. Employers should be willing to invest in their employees' wellbeing and mental health. Glitch provides training on Digital Citizenship, Online Active Bystander and Digital Self Care and Self Defence.

Soft copy can be found on our website fixtheglitch.org