



GETTY

STAYING SAFE ON SOCIAL MEDIA

How scientists can sidestep online harassment or reduce its impact. **By Bianca Nogrady**

The United States Marine Corps could hardly be described as ‘cowards’. Yet that’s exactly the accusation that was levelled at the force last year, when its training facility in San Diego, California, announced on Twitter that it was accepting its first cohort of women – and then immediately switched off comments on the tweets. Such announcements often attract misogynistic and abusive comments. Far from being cowardly, blocking these was smart and strategic, says Imran Ahmed, founder and chief executive of the Center for Countering Digital Hate (CCDH), a non-profit organization based in Washington DC. “Why would they

open up a channel for those people opposed to their fundamental values to attack them?” he asks.

It’s a question that many scientists who work in politically or socially charged fields are now grappling with. For example, the COVID-19 pandemic has been accompanied by an unprecedented ‘infodemic’ of misinformation, disinformation and conspiracy theories concerning everything from the origins and spread of the coronavirus SARS-CoV-2 to infection, prevention and treatment. Alongside this has come a surge in online abuse, harassment and attacks on scientists and health experts.

This abuse has had a chilling effect on the scientists’ ability and desire to communicate their work, not just to the media and the public, but even among themselves in public-facing forums such as social media. And that’s exactly what the people behind online abuse are trying to achieve, Ahmed says. “At a very simple level, trolling is purposeful behaviour, and the purpose of it is to dissuade the target from speaking out freely.”

Scientists have become targets because of their important role in society, and not just during the pandemic, Ahmed argues. “You’re being targeted not because they believe that you’re bad, but because they know that you’re

good,” he says. Online harassers seek to diminish the weight of knowledge and persuasive power that scientists hold, he says.

Online and digital harassment has had a significant impact on scientists working on issues such as climate change, gun control, vaccines and even challenging health conditions such as myalgic encephalomyelitis/chronic fatigue syndrome. But when *Nature* conducted its own research into the abuse of scientists during the pandemic (see *Nature* 598, 250–253; 2021), it found that many researchers interviewed had never encountered such attacks before, and had not expected to attract a lot of vitriol.

Academics are increasingly aware of the risk of becoming a target online, says Edd McCracken, head of news at the University of Edinburgh, UK. When he started working in media and communications in 2011, academics’ main concern was being misrepresented by the media. “Now, people are asking about online abuse,” he says. “It’s affecting people’s willingness to be a public figure and share their expertise.”

The US Marines might have stopped the argument before it began, but scientists and their institutions don’t necessarily have – or want to take – that option. Instead, they must work out how to navigate their online existence to prevent, avoid or mitigate online abuse. As social media has been weaponized wholesale against groups such as female video gamers, women of colour, the queer community and journalists, organizations have arisen to combat that abuse and to aid people who are attacked. Scientists and their institutions can learn from them.

Debate or abuse?

Paediatric infectious-diseases specialist Alasdair Munro at the University of Southampton, UK, was shaken to find that some of the Twitter users who made abusive comments about his research and communication on COVID-19 in children weren’t hiding behind anonymity. “You expect trolling from the public and angry people,” Munro says. “But what I’ve been really surprised about is identifiable senior academics on Twitter behaving in ways that seem so unprofessional and sometimes rude and borderline abusive.”

Cyberpsychology researcher Evita March at Federation University Australia in Melbourne is not surprised by bad online behaviour. She studies the online effect of ‘visual anonymity’. “Our empathy and sharing that emotional experience of others is very dependent on being face to face,” March says. The lack of that face-to-face interaction on social media can therefore create an empathy deficit. And the pandemic has contributed the extra factor of stress. “The more that we experience stress and frustration, the more likely we are to behave antisocially,” March says.



Imran Ahmed at the Center for Countering Digital Hate, advises against engaging with trolls.

Science is no stranger to heated debate, nor to being challenged, questioned and analysed, and that process is fundamental to scientific integrity. So, when does query, challenge or disagreement cross the line into harassment, abuse or trolling?

March says an intention to harm is the biggest red flag. “It could be explicit, as in, ‘I’m going to come and get you and your family,’” she says. It can also be less explicit: the intention to harm psychologically, to upset someone, damage their reputation or make them fear for themselves. “When the intention becomes malicious – that is where we should draw the line,” she says.

“The people who are disproportionately targeted are the ones who are the most silenced.”

However, interactions that are intellectually invigorating for one person could be intensely stressful for another, so the line between passionate engagement and abuse is both nebulous and subjective. It’s up to the individual on the receiving end to decide, says Internet researcher Kat Lo, content-moderation lead at Meedan, a non-profit organization in San Francisco, California, that works to improve digital literacy and tackle misinformation. “If it impacts your quality of life, I think that’s when you should get help.”

Some defined and easily recognized forms of online abuse are listed in guidance from OnlineSOS, a San Francisco-based non-profit group that provides resources for people experiencing online harassment, and for which Lo acts as a research adviser (see go.nature.com/3t5ibij). For example, mob harassment is

when someone is bombarded with messages – such as e-mails, phone calls or social-media comments or tags – that are intended to cause distress or to discredit the target. Other abuse might be explicit or implicit threats of harm, including gender-based or sexual violence, sometimes accompanied with violent or graphic imagery.

Another abusive tactic is doxxing, the public sharing of personal information such as address and contact details, sometimes with a threat that the harasser or others will contact the target in person. There is also the distribution of intimate images without consent, and the spreading of false information that can harm a person’s reputation.

Protect assets and mindsets

People dealing with online abuse used to be told to ‘just log off’. Most advice has come a long way since then, although Lo says that this attitude can still be encountered from institutions and law enforcement. “By saying, ‘well, you can log off’, the people who are disproportionately targeted are the ones who are the most silenced,” she points out.

When engagement becomes overwhelming or abusive, there are a range of things that people can do (see ‘Take action to avoid and mitigate abuse’). OnlineSOS breaks its advice down according to type of harassment, but recommends contacting the police if you have any concern about your immediate safety.

Lo recommends reinforcing security around your digital accounts and data, to reduce the risk of being doxxed or having your digital accounts hacked. It’s also important to evaluate how private your social-media accounts are, what information people can access from them and how accessible you are.

You can search for your personal information online and remove it where possible. If

you or your institution can afford it, a more thorough approach is to pay a data-broker removal service, which might cost around US\$200 per year. “The idea of having to get up and move somewhere else if you don’t feel safe, or just the cost of never feeling totally safe knowing your address is out there, I think it’s incomparable,” Lo says.

It’s tempting to think one should turn and face the challenge. But Ahmed – who, with Linda Papadopoulos, chair of the CCDH advisory board, produced a 2019 guide for public figures called ‘Don’t Feed the Trolls’ – says trolls are hoping people will take them on. “How is it cowardly to not do what malignant actors desperately want you to do?”

And despite the shift away from telling people to log off, Nicolle White, social-media well-being adviser at the Australian Broadcasting Corporation in Sydney, says it’s important to recognize that it’s OK to take a break from the online world and recover. “Ultimately, you need to prioritize your well-being,” she says. “If that means stepping away for a short or a long amount of time, then that’s absolutely something people should do.”

Institutional responsibilities

Most universities have social-media policies. But Jack Heinemann, a geneticist at the University of Canterbury in Christchurch, New Zealand, who has a strong interest in academic freedom, says those policies are often more concerned with limiting what academics can say than with empowering them to feel safe when they’re communicating opinions – even contentious ones.

“A university should be seen as the place you go to talk about controversial and unpopular topics,” Heinemann says. He argues that universities bear a responsibility to ensure that their staff can practice academic freedom safely. “I wouldn’t even put it in terms of doing something to keep us safe – it’s doing things to make sure that we can deliver.”

Unfortunately, the evidence from *Nature’s* previous reporting on abuse of scientists suggests most institutions do not have policies ensuring that the virtual workplace is safe for their staff. But Liz Lee, founder and board chair of OnlineSOS, says that during a period of online abuse, institutional backing – such as a public or internal statement of support – can help significantly.

March experienced this at first hand when she wrote an article criticizing Donald Trump while he was US president. The article attracted a lot of online attention, to the point at which March contacted the social-media team at her university and said she would understand if it wanted to take the article off its website. “They responded and said, ‘No, we stand behind our researchers,’” March recalls. “That is just so empowering; you feel like you have a safety net.”

White says that because “online abuse really does aim to isolate”, institutions can help by connecting people experiencing harassment with peers who have already been through it. At the University of Edinburgh, McCracken and his colleagues consulted academics who had experienced online abuse to ask how the university could best support them and others in future.

In response, the institution has made it easier to remove a staff member’s contact details from its website, and sometimes provides extra staff to help screen messages. If a staff member is being threatened or intimidated online, there is a system for them to work with the university’s security department – and the police, if needed.

McCracken and his team include social-media training in their general media training. This covers advice on “curating your space, really understanding the physics of social media – how it works, how it amplifies heat, but not so much light,” McCracken says.

Lee notes that online abuse can be traumatizing for its targets. It might also be difficult for someone to articulate why abuse is distressing for them. It’s therefore key that institutions believe people who report online abuse, and that they don’t act dismissively or lay blame on the target. “There are early messages and narratives that I think could be really detrimental,” Lee says, because a lack of support can compound trauma.

Pre-emptive prevention

The best way to mitigate online abuse is through measures to prevent it happening in the first place. Lee says it’s worth taking an approach similar to what investigative journalists do before publishing a major piece. This is called threat modelling, and includes “thinking about what you’re most concerned about, what you would like to protect, and if something were to happen, what action you would like to take”, she says.

Many of the actions that are recommended in response to online abuse can be put in place before it happens – increasing the security of online accounts, limiting comments on posts, removing contact details or setting up a post-office box instead of giving out your address.

Lo suggests that the costs of these safety measures should be built in to a research endeavour from the beginning, to avoid researchers having to pay out of their own pockets for harassment protection and clean-up. “If your research might be risky when it gets published, then, in the grant proposal, budget funding for data-broker removal services,” she says.

Munro also advocates that scientists become agents of change by being good online citizens themselves. He argues that they can avoid discourse that devolves into a “dumpster

Take action to avoid and mitigate abuse

There are many steps scientists can take to prevent online harassment, or to combat it and reduce its impact.

- Set up two-factor authentication on as many of your online accounts as possible: social media, finance, cloud services and so on.
- Use a password manager to create strong passwords for your accounts.
- Check the direct-messaging settings for your social-media accounts and limit who can reach you.
- Get a friend to review what the general public can see on your social-media accounts.
- Do a search to see what personal information (such as your address, telephone number, e-mail address) is available online, or pay a data-broker removal service to find and remove this information.
- Ask your institution to remove your contact details from its website.
- Review and make use of social-media safety options, such as muting and blocking certain accounts, reporting abusive accounts, turning off comments on your posts, preventing others from tagging you and removing yourself from conversation threads.
- If abuse is overwhelming you, get a friend or colleague to help screen your e-mails and messages.
- Document abusive messages by using screen shots or printing them out.
- Don’t retweet or share abusive messages or posts. Ask friends and contacts to refrain, too.
- Don’t be afraid to step away and log off to look after your mental health.

fire” by not tweeting while angry, being aware of power imbalances, not taking screenshots of or sharing other people’s posts without them knowing and focusing on the issue rather than the individual.

Ahmed says it’s important to boost science communication itself, rather than tangle with trolls and abusers. “Every hour that you spend debating someone, arguing in bad faith, is an hour that could have been spent amplifying and engaging with good content,” he says. “Engage with science, not with misinformation.”

Bianca Nogrady is a freelance journalist based near Sydney, Australia.