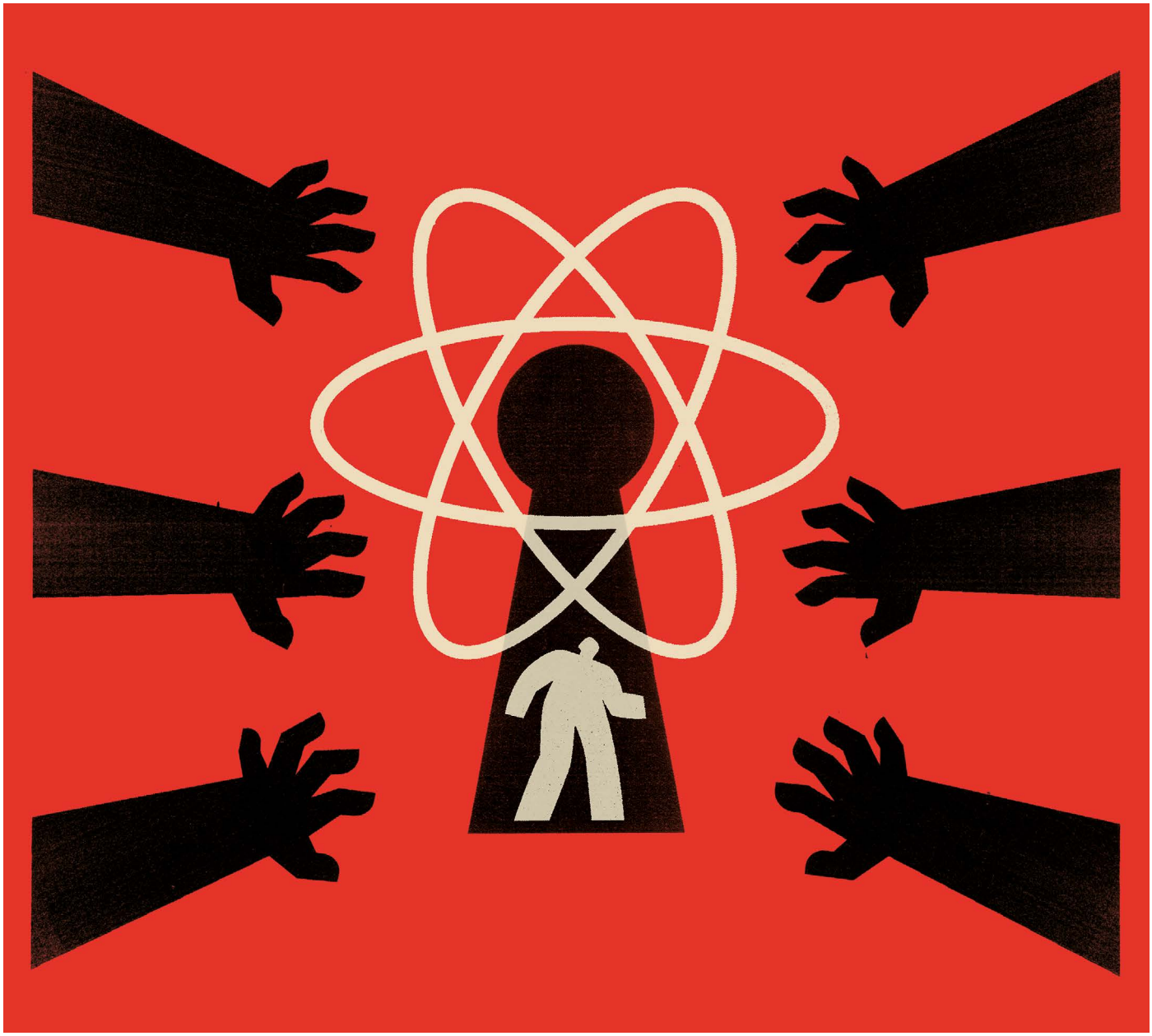

ILLUSTRATION: THE PROJECT TWINS

SIX STEPS TO PROTECT RESEARCHERS' DIGITAL SECURITY

Many US scientists have reported a rise in targeted harassment. Here are tools and tips to safeguard your cybersecurity. **By Virginia Gewin**

Academics around the world are increasingly under fire. In January 2025, the American Association of Colleges and Universities published a survey that found that 53% of US faculty members were worried that their work would make them targets of harassment (see go.nature.com/493upmy).

The Free to Think 2025 report by the Scholars at Risk network described a "global crisis for academic freedom", documenting 395 attacks on scholars and academic institutions in 49 countries, including the United States and Germany, between 1 July 2024 and 30 June 2025 (see go.nature.com/4jk4cI6).

Now, one year into Donald Trump's second term as US President, anti-science rhetoric and attacks show no sign of abating – both in the United States and elsewhere. In the United States, the federal government took steps to control university admissions, hiring and free-speech policies. In response to political pressure, individual researchers and entire departments have reported having to purge any mentions of diversity, equity and inclusion (DEI) from grant applications and websites. The European Parliament conducts an annual

Academic Freedom Monitor report; the 2024 version found that "the state of *de facto* academic freedom across the EU continues to erode", owing to such forces as changing political systems, intensifying geopolitical tensions and the growing use and impact of social media (see go.nature.com/4subrrf). One blog post by the Alexander von Humboldt Institute for Internet and Society in Berlin notes that "disinformation researchers across Europe are being sued, harassed and publicly smeared simply for doing their job" (see go.nature.com/4q45auq).

It's difficult to track how many academics have been targeted. "It's very under-reported. As a result, these attacks leave people isolated," says Beck Haberstroh, digital-safety training manager at PEN America, a non-profit organization in New York City that defends free expression. In June 2025, the organization held a workshop to train scientists on how to combat harassment. "Normally, our workshops are 20–50 people; that workshop, we had more than 300," Haberstroh says. "It's been an intense year."

Harassment can take many forms, such as doxxing (maliciously publishing someone's private or personally identifiable information). Some researchers also receive huge numbers of Freedom of Information Act (FOIA) requests, which some think are being weaponized to challenge or censor researchers working on politically sensitive topics, by slowing down their work by making them respond to requests, including those asking to see their personal messages. The University of Virginia in Charlottesville reportedly received 849 FOIA requests from 1 January to 5 November 2025 — up from 786 in 2024 (see go.nature.com/48gtnwa).

Students in the United States are also increasingly making surreptitious recordings of lecturers in the classroom and posting them on social media, where the videos can become fodder for politicization.

There are even 'watch lists' of allegedly 'left-leaning' professors (see go.nature.com/4q6yho2). After the fatal shooting of US conservative activist Charlie Kirk last September, there was an increase in circulating watch lists of faculty members and scholars to target, says Isaac Kamola, who studies the politics of higher education at Trinity College in Hartford, Connecticut. As of early December 2025, David Langkamp, a programme coordinator at the American Association of University Professors in Washington DC, had documented 52 incidents of sanctions — including suspensions and investigations — imposed on faculty members in the wake of Kirk's death.

Researchers working in politically charged areas, or who are active on social media or in public discourse, are on the front lines of harassment and intimidation campaigns. One climate scientist who spoke to *Nature* on the condition of anonymity has taken a variety of remarkable, unorthodox steps to protect themselves in recent years. Their office location is not shared online and they've taken their name off the door. They've also set up alerts for their name on the Dark Web, created Google alerts for their name, address and phone number, and moved their climate discussions to the California-based encrypted messaging app, Signal. Their near-term security goal is to pay off their mortgage as soon as possible so that they can list their home in an independent trust to protect their address.

> **"Every time you order food, you are spraying data into the world."**

Nature spoke to Kamola, Haberstroh and other privacy specialists about basic steps that academics can take — as well as technology and tools they can use — to better protect their digital security. Here are their key recommendations.

Assess your risk

"Everybody should start with a risk assessment," Kamola says. Consider the spectrum of digital vulnerabilities — outdated software, weak passwords, cloud services and social-media profiles — then take steps to mitigate the risks.

Step one is simple: "It's a good practice to set up a Google alert for your name," says Haberstroh. That will help to flag, for example, new mentions on websites or watch lists.

But also think about the many ways in which you can leave a digital fingerprint. Platforms such as LinkedIn and the US mobile-payment service Venmo "can leak a lot of personal information", says Haberstroh. So too can food-delivery apps: "Every time you order food, you are spraying data into the world," says Aaron Roussell, a sociologist at Portland State University in Oregon. He advises individuals to pare back on unnecessary digital services because these can vary wildly in their data-protection protocols.

Keep personal data personal

Be aware of laws that can apply to your research and teaching. In the United States, "if you work for a public university, anything that you put in writing that is transmitted to another person using channels such as e-mail, or stored on your university's licensed version of Dropbox, might be FOIA-able or can be made available to the federal government", explains Britt Paris, an information scholar at Rutgers University in New Brunswick, New Jersey, "so be careful".

In other words, keep personal information in your personal e-mail. If a university e-mail address is the target of a FOIA request, anything in your archive — be it about public university business or personal health or court documents — can become public record, says Roussell.

Encrypt your communications

If privacy is a concern for your e-mail and messaging, consider encrypted options such as Signal, Riseup and the Switzerland-based e-mail company Proton Mail. Riseup is a non-profit organization that offers privacy-focused e-mail, a virtual private network (VPN) and other collaboration tools for secure communication. If you're worried that someone could be tracking your phone, a VPN — or even just restarting your phone at regular intervals — can reduce your risk, says Roussell.

It is also worth exploring encrypted alternatives to popular collaboration tools. Roussell says that some video-conferencing platforms' privacy and security concerns have prompted some individuals to switch to Jitsi, an encrypted, open-source (and free) alternative. As with Signal, the online meeting room disappears once the meeting is over. Similarly, instead of Google Docs and Sheets, some researchers prefer CryptPad, an encrypted, open-source suite of spreadsheets, whiteboards and text tools, that lets users edit files simultaneously.

Whatever apps you choose, Haberstroh and others encourage using a unique, long password and two-factor authentication when possible. Use a password manager such as 1Password to keep your login details organized.

And consider a YubiKey, a physical dongle that plugs into your computer's USB port to unlock specific files or accounts. "That's the most secure form of two-factor authentication," says Haberstroh. It's not necessary for everyone, but "particularly in the last year, we're seeing more situations where academics working on higher-risk topics are using YubiKey".

Clean up your digital footprint

At the PEN America workshop, Haberstroh teaches attendees how to effectively dox themselves. "We try to think like a doxxer would," they explain. Step one: google yourself to see what data might be floating around. Personal information, including phone numbers, addresses and even family trees, are collated regularly by data brokers who scrape data from websites and organize it online for a price.

Step two: delete data that you don't want out there. "Individuals can manually delete their data but it's time-consuming," says Haberstroh. "It's a bit like the game 'Whack-a-mole'." They suggest setting aside time every six months to scrub data. "Even if you opt out of a website once, six months to a year later,

your information can be scooped up and put back online," Haberstroh explains. This is true in the United States, at least; Europeans have greater protections against those practices (see go.nature.com/45ze06f).

Alternatively, services such as DeleteMe, EasyOptOuts and Optery can scrub your personal data from online data brokers for a fee. DeleteMe, for instance, costs roughly US$130 per year. That said, no data scrubber is perfect, says Haberstroh. The non-profit consumer organization Consumer Reports compared data-scrubber services in 2024 and found that EasyOptOuts offered the best results for the lowest price (see go.nature.com/44w6ptx). "Put your data in third-party hands that you trust," advises Roussell. Organizations that have all of your information but lack good security are high risk. "Bad security is worse than no security," he says.

Other tools can give your social-media accounts a deep clean. For example, the California-based software firm Block Party can optimize privacy settings, delete old posts and photos, and even filter abusive content into a lockout folder so that users don't have to see it.

Scrutinize institutional privacy

Check with your information-technology department to see what cybersecurity software it recommends and supports. But remember that even these tools could pose risks. Last June, privacy concerns among University of California faculty members across all ten campuses prompted the academic senate to pass a resolution to halt the implementation of Trellix cybersecurity software. Critics alleged the software threatened research integrity and academic freedom because government agencies might be able to access data, and files could be altered without user consent. In the wake of student protests, a massive surveillance infrastructure has been put into place by universities and politicians that can be weaponized against people or views that the government disagrees with, asserts Lilly Irani, a communication researcher at the University of California, San Diego.

"Organizations that have all of your information but lack good security are high risk."

Build a community

Finally, remember that you don't have to be alone. "I can't overemphasize the importance of community," says Roussell. He advises academics to maintain an active conversation with their colleagues around digital security.

Several initiatives have formed over the past few years to provide researchers with support, tools and guidance for managing their online safety. Scholars at Risk Europe advocates for policymaking to protect researchers and increase respect for academic freedom across the world. Expert Voices Together launched in 2025 to support individuals during intense moments of harassment and intimidation, says co-founder Rebekah Tromble, who is director of global partnerships at the Institute for Information, the Internet and Democracy at Northeastern University in Boston, Massachusetts. Expert Voices Together offers digital and security support, as well as connections to legal and mental-health resources. The Researcher Support Consortium, also co-created by Tromble, offers guidance and toolkits for both individuals and their institutions to combat intimidation and harassment attacks.

In 2020, Kamola formed another option, Faculty First Responders, to advise academics facing online harassment and attacks. "We regularly meet with faculty who are facing targeted harassment to provide peer-to-peer support", he says, "because the experience of targeted harassment can be incredibly alienating." But with the proper tools, practices and community, it doesn't have to be.

Virginia Gewin is a freelance writer in Portland, Oregon.

Corrected 27 January 2026

Correction
This technology feature misstated Lilly Irani's research field.

Corrected 27 January 2026