CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

5 MINUTE READ

GENERAL

Staying Safe:
Protecting You and Your Research

Researching national security, geopolitics, extremism, or other politically sensitive issues can expose you to risks that most academics never have to consider.

> **Above all, remember: if you are targeted, it is not your fault.**

INTRODUCTION

Researching national security, geopolitics, extremism, or other politically sensitive issues can expose you to risks that most academics never have to consider. The very activities that make your career successful, pursuing challenging topics, engaging with people online or in the field, publishing widely, and building networks, may also make you vulnerable to unwanted attention.

This guide is designed to help you assess your exposure, understand the kinds of threats you may face, and take realistic steps to protect yourself. It is not about becoming paranoid or cutting yourself off from your research community. Rather, it is about recognising that threats exist, and aims to show you how to put in place habits and protections that will keep you, your work, and your networks as safe as possible.

Good digital hygiene doesn't just protect you from targeted threats; it also helps you avoid the more routine risks that affect everyone, such as online fraud, identity theft, and crime-based phishing. The same practices that make you safer as a researcher will also strengthen your overall online security.

Above all, remember: if you are targeted, it is not your fault. Even the most careful researcher can experience harassment. Safety is not about personal failure or paranoia, but about building resilience in a world where digital and political risks are part of everyday academic life.

WHY RESEARCHERS ARE VULNERABLE

Success in academia often depends on visibility. Publishing in high-profile journals, attending conferences, engaging with policymakers and practitioners, and sharing your work online are all important for building a career. Yet this visibility also highlights you and your research to those who may wish to misuse, undermine, or discredit it.

Hostile actors, whether extremists, state-linked organisations, organised crime groups, or even online subcultures, may take an interest in your work. They might seek to compromise your accounts, damage your reputation, or recruit you under false pretences. At the same time, your personal networks, such as family and friends, can inadvertently expose information that makes you easier to target.

The risks are layered and multi-channelled. Some threats are direct, such as phishing emails or suspicious recruitment offers. Others are more passive, such as the information adversaries can collect from your public profile, past publications, or media appearances. Sometimes the risks spill over onto those closest to you, through doxing or attempts at emotional leverage.

UNDERSTANDING RISK

Anyone conducting research on sensitive or controversial topics may be at risk. You do not need to hold security clearance or work directly with government to become a target. Researchers in universities, think tanks, NGOs, or industry can all be approached, particularly if their work touches on terrorism, extremism, radicalisation, human rights, marginalisation, or emerging security technologies.

Certain details may increase your visibility. Publicly identifying yourself as connected to government or sensitive industries, mentioning security clearances, or listing specialist expertise can all attract unwanted interest. Similarly, researchers from a marginalised community or those with a protected characteristic may be more vulnerable, especially when combined with politically charged research topics.

Hostile actors often appear professional and legitimate. They may pose as recruiters, journalists, or potential collaborators, slowly drawing you into conversations that seem harmless but are designed to gather information. They may use flattery, urgency, or offers that feel “too good to be true” to encourage you to respond.

HOW ADVERSARIES OPERATE

The tactics used to target researchers vary, but they often fall into two main categories.

Some actors create entire cover organisations, complete with websites and fake staff profiles, to build credibility.

The first is **gaining access**. This can involve fake job offers, invitations to speak at conferences, or recruitment approaches on professional platforms such as LinkedIn. Some actors create entire cover organisations, complete with websites and fake staff profiles, to build credibility. Over time, they may try to move conversations onto encrypted platforms or request meetings abroad.

The second is **undermining research**. Here, the goal is to discredit or intimidate. This may take the form of phishing emails that compromise your accounts,

surveillance of your online activity, or coordinated campaigns to smear your reputation. In some cases, adversaries release personal information publicly, known as doxing, in an attempt to silence or intimidate you.

In both cases, the aim is to either exploit your research access or diminish your credibility a deliberate strategy to instill fear and discourage participation. The outcome may be subtle, such as gradually shifting your research priorities or sharing seemingly innocuous details of your contacts, or more visible, such as reputational attacks in the media or online.

BUILDING DEFENSIVE PRACTICES

While no set of actions can remove risk entirely, small changes can significantly reduce your exposure.

DIGITAL HYGIENE

The first step is strengthening your digital hygiene. Use strong, unique passwords and enable two-factor authentication on all critical accounts. Treat your email as your most secure gateway, and check whether your details have been exposed in past data breaches via free commercially available sites such as *www.haveibeenpwned.com*. For particularly sensitive work, you could consider using separate devices and making use of applications such as ProtonMail and Signal which offer free, relatively secure messaging.

PUBLIC PRESENCE MANAGEMENT

It is also important to manage your public presence. Search for your name and personal details regularly, and be aware of how your photos and information circulate online via reverse image searching. Audit your social media privacy settings, and consider what information about you is easily discoverable from university or institutional websites. Keep profile photos different across platforms to reduce traceability.

EVALUATE DIGITAL CONTACTS

Be cautious when approached online, particularly by individuals or organisations you cannot verify. Take time to check credentials, cross-reference affiliations, and consider whether the style of communication feels unusual. Flattery, urgency, or insistence on secrecy should always raise questions.

ENHANCE PHISHING AWARENESS

Finally, learn to recognise phishing attempts. Poor spelling, generic greetings, or requests to click unfamiliar links are common warning signs. If something feels suspicious, pause and seek advice before responding.

EXTENDING PROTECTION BEYOND YOURSELF

Risks do not stop with you. Family members, friends, and colleagues can also be targeted as indirect routes to information or intimidation. A child posting a location-tagged photo, or a partner using a shared device, may unintentionally increase your exposure.

Discuss these risks openly with those close to you. Encourage the use of secure communication apps such as Signal or WhatsApp for private conversations, and explain why some precautions, like avoiding location tags, matter. Not everyone will feel comfortable adopting new habits immediately, but creating a shared understanding of risk will strengthen your overall safety.

Within your professional community, cultivate networks of support. Share resources, encourage peers to audit their digital presence, and build collective resilience by normalising conversations about safety.

MOVING FORWARD

Protecting yourself as a researcher is not a one-off task. It is a continuous practice of awareness, reflection, and adjustment. A useful habit is to set regular reminders, perhaps every few months, to review your digital exposure, update passwords, and check how your personal details appear online.

Researchers should not feel they have to manage these risks alone. Departments and universities have a responsibility to support their staff and students, and institutions recognise that researchers can become targets because of the topics they study. Security offices, ethics committees, and supervisors can provide advice and practical help. Organisations such as the National Protective Security Authority (NPSA) and the National Cyber Security Centre (NCSC) also offer specialist guidance. The NPSA's Trusted Research materials include advice for academics travelling overseas, as well as steps to protect research collaborations and data. Increased awareness at university level, combined with good digital and professional practice, can mitigate many of the risks outlined in this guide. Finally, remember that colleagues facing similar challenges can be some of the best sources of practical advice and emotional support. Sharing experiences within trusted networks can help normalise conversations about security and strengthen collective resilience across the research community.

Today, the field of security-related research is far more developed than it was even a decade ago, and that is thanks to the many academics who have dedicated themselves to advancing it. With that growth, however, comes greater exposure and risk. Too often, the personal costs of doing this work are not openly acknowledged.

So this ends with a thank you – to all of you who continue to pursue this vital research, not despite the risks, but often because of them. Your courage and curiosity are shaping the future of this field. The work you do makes a profound difference, and we want you to be able to continue doing it safely.

FURTHER RESOURCES

READ MORE

- Association of Internet Researchers: Risky Research Report https://aoir.org/wp-content/uploads/2025/05/AoIR-Risky-Research-Report_2025.pdf
- Advice for MPs (given their similar need to publicise and protect themselves, and the similar threat) https://www.ncsc.gov.uk/files/NCSC-Advice-for-MPs-keycards.pdf
- Advice for journalists (given the similar threat from anti groups) https://cpj.org/2019/07/digital-safety-kit-journalists/
- Useful tool that creates personalised advice on protecting devices https://medit.med.utoronto.ca/security-planner
- List of useful resources on practical tools for academics to protect themselves https://voxpol.eu/researcher-welfare-1-privacy/
- Think before you link campaign from NPSA delivering advice on social network sites https://www.npsa.gov.uk/security-campaigns/think-you-link-tbyl-0
- Aimed at university students who are overseas https://www.fbi.gov/news/stories/advice-for-us-college-students-abroad
- The risks from state actors – briefing by Richard Horne, CEO of NCSC https://www.youtube.com/watch?v=0yxY633l3c8
- Risks and considerations for academic researchers, largely aimed at protecting IP but there is some relevant advice https://www.npsa.gov.uk/specialised-guidance/trusted-research/trusted-research-academia
- Advice for 'high risk' individuals: Infographic: https://www.ncsc.gov.uk/files/Cyber-security-high-risk-individuals.pdf
- NCSC advice https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_2
- NPSA advice https://www.npsa.gov.uk/specialised-guidance/personal-safety-security-high-risk-individuals
- Vaughan, A. (2025) Researching the Far Right Safely in Academia. VoxPol. Available at: https://voxpol.eu/wp-content/uploads/2025/10/DCUPN0753-Researching-Far-Right-WEB-250814.pdf

Accurate at time of printing, please check for updated guidance.

COPYRIGHT This Briefing is made available under a Creative Commons BY-NC-SA 4.0 licence. For more information on how you can use CREST products see **www.crestresearch.ac.uk/copyright**

IMAGE CREDIT Adobe Stock