Online Harassment Information for Universities

Why am I receiving this information sheet?

This information sheet has been created to help university administration, communications teams, department heads, campus security, and other institution officials respond effectively when a researcher faces online harassment. People can become targets of online abuse for many reasons, ranging from retaliation against published work or perspectives, discrimination (race, gender, sexuality, etc.), continuation of offline abuse, or even a case of mistaken identity. Researchers conducting sensitive or risky research—particularly about controversial topics—may be susceptible to online harassment and related threats. Researchers who maintain high-profile presences on social media sites may also be vulnerable. It is imperative for the health and safety of researchers that institutions be aware of the associated risks, so that they may take appropriate precautions and respond to harassment quickly and effectively.

What is online harassment?

Online harassment is the use of networked technologies to threaten, maliciously embarrass, or attack another individual. It includes behaviors that range from merely irritating to life-threatening. Some typical techniques include "doxing," or revealing personal information publicly; "brigading," or when a group of people work together to harass an individual; "revenge porn," or disseminating private photos (real or falsified) without the individual's consent; and "swatting," or reporting a false threat to local police, prompting an emergency response team to the individual's home. Harassment can often escalate to targeting an individual's friends, families, colleagues, and employers.

Anyone can be harassed online, even if they take every possible measure to protect themselves. It is important not to blame or criticize a person who is experiencing harassment, even if you feel that they could have done more to protect their online safety.

How can we prepare?

One way that individuals may harass a researcher is by bombarding their institution with messages, complaints, and threats—even if empty and without merit—in a coordinated attempt to discredit them or get them fired. Individuals may recruit additional people or create fake accounts to make online harassment look like legitimate public outcry, or to seem like a significant threat to an institution's reputation. Online harassment campaigns can vary widely in terms of scale and duration. They are meant to damage the standing of the researcher within their institution; impede their research; damage their public reputation; or challenge the validity of their work.

Beyond direct harassment of the researcher, examples of online harassment relevant to institutions or universities include: complaints and threats about the researcher to the institution's social media accounts; emails or phone calls to institutional review boards, department chairs, or deans; and harassment of the researcher's colleagues or affiliates. Since information about classes, office hours, and university events is often made public, the researcher's physical comfort and safety may be put at risk, requiring additional safety precautions.

What can we do?

- Have a proactive communications plan for dealing with online harassment, involving university and department public relations and social media personnel.
- Appoint a point person(s) who is knowledgeable about cybersecurity, social media, and harassment whom researchers or students can rely on for support.
- Educate department and university personnel about these issues.
    - Create a one-sheet guide and disseminate it to university employees and students. Include definitions of online harassment, links and contact information for security, counseling services, IT, and relevant resources.
    - *Example: Rutgers University* guide to offline harassment *(PDF)*
- Harness university resources (e.g., IT, campus police) to protect the researcher: filter email accounts, secure websites, provide additional security (if necessary), etc.
- Do not give out any additional information about the researcher(s) without their explicit consent and communicate suspicious activity to them if requested.
- Investigate the merit of claims or threats and discuss them with the researcher for further context and clarification before acting.
- Acknowledge that online harassment is a real and significant problem, and cannot be solved by simply "staying off the internet." (A helpful analogy: if a student were being stalked, would you suggest they never go outside?) Pulling back from online engagement can be especially damaging for researchers, whose online presence is often important for their careers.
- Recognize the psychological harm that can result from online harassment and make emergency counseling services available, should harassment occur.

Read Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment for more resources on protecting and supporting researchers facing online harassment.

Adapted from Crash Override's guide for employers of targets of online harassment