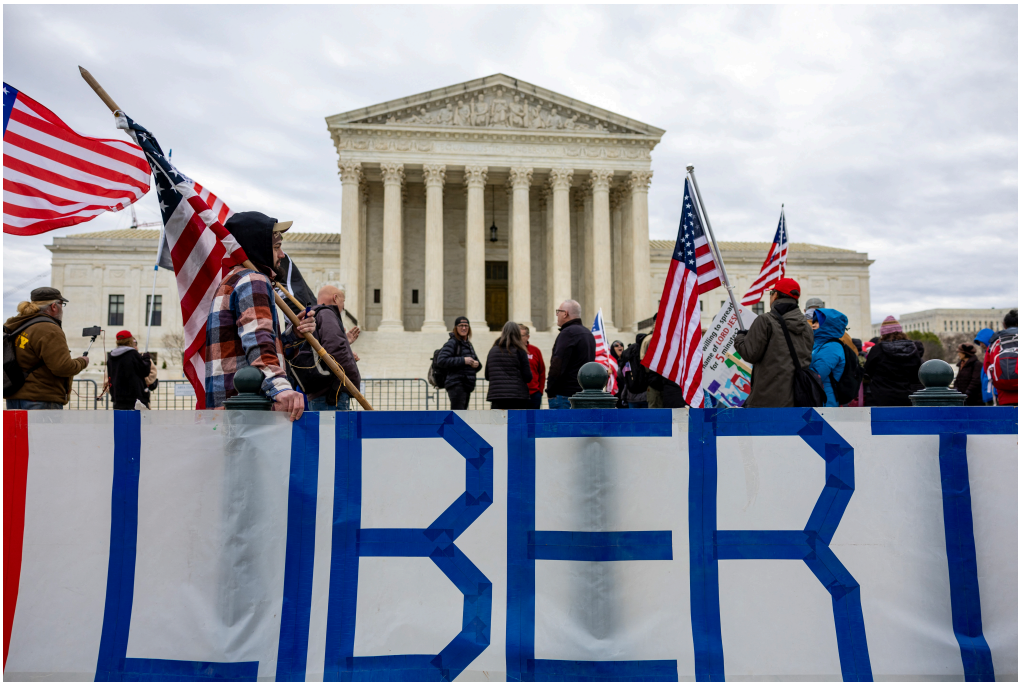
Committee to Protect Journalists

U.S. Presidential Election 2024: Journalist safety kit



Supporters of the protesters who were arrested in the January 6, 2021 attack on the U.S. Capitol gather outside the U.S. Supreme Court in Washington, D.C., on the second anniversary of the insurrection. (Photo: Getty Images / Tasos Katopodis / Getty Images via AFP)

The 2024 United States presidential election will take place on Tuesday, November 5 amid an increasingly polarized political climate. In addition to facing a high level of distrust in the media, journalists are likely to confront significant security challenges in the lead-up to the election, as well as on election day.

The contested 2020 election and the January 6, 2021 attack on the U.S. Capitol have contributed to a rise in domestic extremism and an increased presence of politically motivated militia groups, who are likely to appear at political rallies and polling stations in certain U.S. states. As a result, journalists may face forceful reprisals, including physical harassment, obstruction, and verbal abuse. Media workers covering the election should be aware of the increased risk of online abuse, including doxxing, and targeted disinformation campaigns designed to undermine the press. This underscores an increasingly hostile environment for journalists in the U.S., with at least 40 assaults against journalists in 2023, according to the U.S. Press Freedom Tracker, a comprehensive database of U.S. press freedom violations, of which CPJ is a founding member.

The guide below is designed to help newsrooms and journalists think about and manage physical and digital risk when it comes to covering the U.S. election.

Committee to Protect Journalists

Contents

Committee to Protect Journalists

Editors' Checklist

For journalists, having a quick conversation with their editor can increase risk awareness and enhance your safety. The following checklist enables editors to best prepare journalists and other media workers as they cover election hotspots or risky assignments.

When selecting your reporting team, consider:

- How experienced are the journalists?
- Have they covered stories with elevated tension or emotions that can lead to violence?
- Do they have a history of good decision-making under pressure?
- If they are less experienced, what support mechanisms can you put in place to increase their safety? For example, could a more senior journalist cover the desk and provide guidance if needed?
- Is your team mentally prepared to be confronted by aggressive individuals?
- On higher-risk stories, can you assign two journalists, so no one works alone?
- Bear in mind that exposing the identity of the journalist may increase their risk of harm, and plan accordingly. In some cases, a journalist's identity may also help to keep them safe.
- Do they have local knowledge about the area they will be working in?

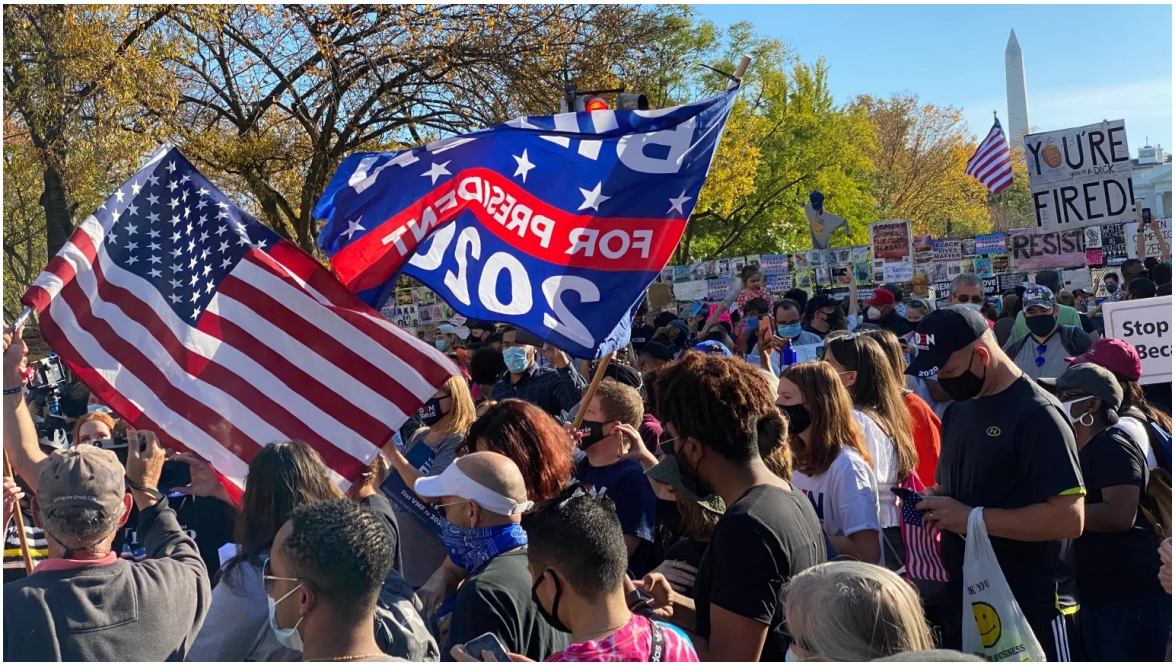
As part of your risk assessment, discuss:

- Establishing a check-in procedure.
- What footage or other material will be needed to complete the assignment. There is no point lingering at a risky crowd event gathering material that will not be used.
- Conducting a dynamic risk assessment and consider using CPJ's risk assessment template.
- The potential for online attacks as a result of reporting on the election. Review CPJ's editor's checklist on protecting staff and freelancers against online abuse.
- What indicators to look for that would trigger a withdrawal of the team from their reporting location.
- Recording the emergency contacts and details of all staff being sent on the assignment.

To increase awareness when in the field, advise journalists to:

- Consult CPJ's safety guide for journalists on utilizing situational awareness.
- Maintain a low profile and gauge the mood of crowds toward the media before entering any situation. Always use discretion when reporting or filming, especially around people who are armed or aggressive.
- Plan for regular check-ins with your editor or newsroom point of contact. If working as a freelancer, consider having a check-in procedure with a fellow journalist, family, or friend.

- Ensure that your mobile phone is fully charged. Consider taking a power bank with you.
- Take the time to plan an exit strategy in case the situation turns violent. Identify where you can take cover if you are able to escape, or until help arrives.
- If you are working alone or after dark, be extra vigilant, as the risk potential increases.
- Avoid individuals who are under the influence of drugs or alcohol.
- If possible, try to build a rapport with individuals before interviewing them.
- When conducting an interview, consider your situation. Are you surrounded by others who may take an interest in your reporting? It is often individuals on the periphery who start causing trouble, rather than interviewees.
- When you are on the phone or filing copy or footage, ensure that you are in a protected space where you can see threats coming.
- In general, be prepared to be verbally abused, intimidated, or even spat at. Remain calm and do not allow yourself to be provoked.
- Consider your choice of clothes. Avoid wearing flammable materials, such as nylon, or anything that is loose-fitting and can be grabbed. Avoid newsroom logos and political slogans, as well as military fatigues and black-colored outfits, which are often worn by far-left anti-fascist (antifa) groups.
- If an incident occurs, take notes on what happened and notify the relevant authorities.
- Continuously observe the mood and demeanor of the authorities. Visual cues such as police in riot gear, shield walls, or thrown projectiles are potential indicators that aggression can be expected. Pull back to a safe location when such "red flags" are evident.
- In general, be prepared to leave the situation if you feel the level of risk escalating or that appealing to the authorities would be to no avail.
- If you leave, retreat to a safe location before reporting into your newsroom or point of contact.



People gather at the Black Lives Matter Plaza across from the White House in Washington, D.C. on November 8, 2020. (Photo: Daniel Slim / AFP)

Physical Safety: Covering election rallies and events

The killing of George Floyd and Breonna Taylor in 2020 brought to light the public and violent disregard for journalism by police. The police failed to uphold basic constitutional rights for journalists, leading to unjust arrests and suppression tactics at big and small protests, according to a 2023 report from the Knight Foundation.

To minimize risks when covering election rallies and events:

- Plan the assignment and know the area where you are going. Work out in advance what you would do in case of an emergency. Take a medical kit if you know how to use it.
- Ensure that your phone has a fully charged battery. Consider if you should take a power bank.
- Wear clothing without media company branding and remove media logos from equipment/ vehicles if necessary. Have appropriate clothing and footwear.
- Always try to work with a colleague and have a regular check-in procedure with your base, particularly if covering rallies or crowd events.
- Wear clothing and footwear that allows you to move swiftly. Avoid loose clothing and lanyards that can be grabbed, as well as any flammable material (i.e., nylon).
- Consider your position. If you can, find an elevated vantage point that might offer greater safety.

- At any location, always plan an evacuation route as well as an emergency rendezvous point if you are working with others. Know the closest point of medical assistance.
- Maintain situational awareness at all times and limit the number of valuables you take. Do not leave any equipment in vehicles, which are likely to be broken into. After dark, the criminal risk increases.
- If working in a crowd, plan a strategy. It is sensible to keep to the outside of the crowd and don't get sucked into the middle where it is hard to escape. Identify an escape route and have an emergency meeting point if working with a team.
- Photojournalists generally have to be in the thick of the action, so are at more risk. Photographers should have someone watching their back and should remember to look up from their viewfinder every few seconds. Do not wear the camera strap around your neck to avoid the risk of strangulation. Photojournalists often do not have the luxury of being able to work at a distance, so it is important to minimize the time spent in the crowd. Get your shots and get out.
- All journalists should be conscious of not outstaying their welcome in a crowd, which can turn hostile quickly.
- Consider the need for security if the risk is high. A local hired back watcher to protect you/ your kit can be attuned to a developing threat while you are concentrating on work.
- Police in the United States have used tear gas, batons, pepper balls and rubber coated bullets to disperse crowds. Consider using personal protective equipment, but if this is not appropriate, pay attention to the police. If firearms are visible, move to hard cover and do not dwell in natural exits in case of a stampede.

To minimize the risk when dealing with tear gas:

- You should wear personal protective equipment that includes a gas mask, eye protection and respirator.
- Individuals with asthma or respiratory issues should avoid areas where tear gas is being deployed. Likewise, wearing contact lenses is not advisable. If large amounts of tear gas are being used, there is the possibility of high concentrations of gas sitting in areas with no movement of air.
- Take note of any potential landmarks (i.e., posts, curbs) that can be used to help you navigate out of the area if you are struggling to see.
- If you are exposed to tear gas, try to find higher ground, and stand in fresh air to allow the breeze to carry the gas away. Do not rub your eyes or face, as this may worsen the situation. Once possible, shower in cold water to wash the gas from skin, but do not bathe. Clothing may need to be washed several times to remove the crystals completely or even discarded.

Physical Safety: Dealing with aggression

- Read people's body language, and use your own body language, to pacify a situation.
- Maintain eye contact with an aggressor, use open hand gestures, and talk in a calming manner.
- Keep an extended arm's length from the threat. If someone grabs you, break away firmly without aggression. If cornered and in danger, shout.
- If the situation escalates, keep a hand free to protect your head and move with short, deliberate steps to avoid falling. If part of a team, stick together and link arms.
- Be aware of the situation and your own safety. While there are times when documenting aggression can be newsworthy, taking pictures of aggressive individuals can escalate a situation.

Physical Safety: Dealing with armed extremists

Militia groups have made their presence felt within the American political environment in recent years. Most groups oppose government and law enforcement powers, though some view themselves as potential partners to certain law enforcement agencies. A report by ISD Global states that extremist ideologies have constantly evolved over the past two decades and a new younger generation of extremists have emerged. This can be attributed to the use of online platforms being used to reach broader audiences and to push extreme ideologies into the mainstream.

ACLED research shows that the Three Percenters, Proud Boys, Patriot Prayer and Boogaloo Bois have a high or very high history of using violence during elections. Since the 2020 election, far-right militias have been involved in 91 percent of violent demonstrations, according to ACLED.

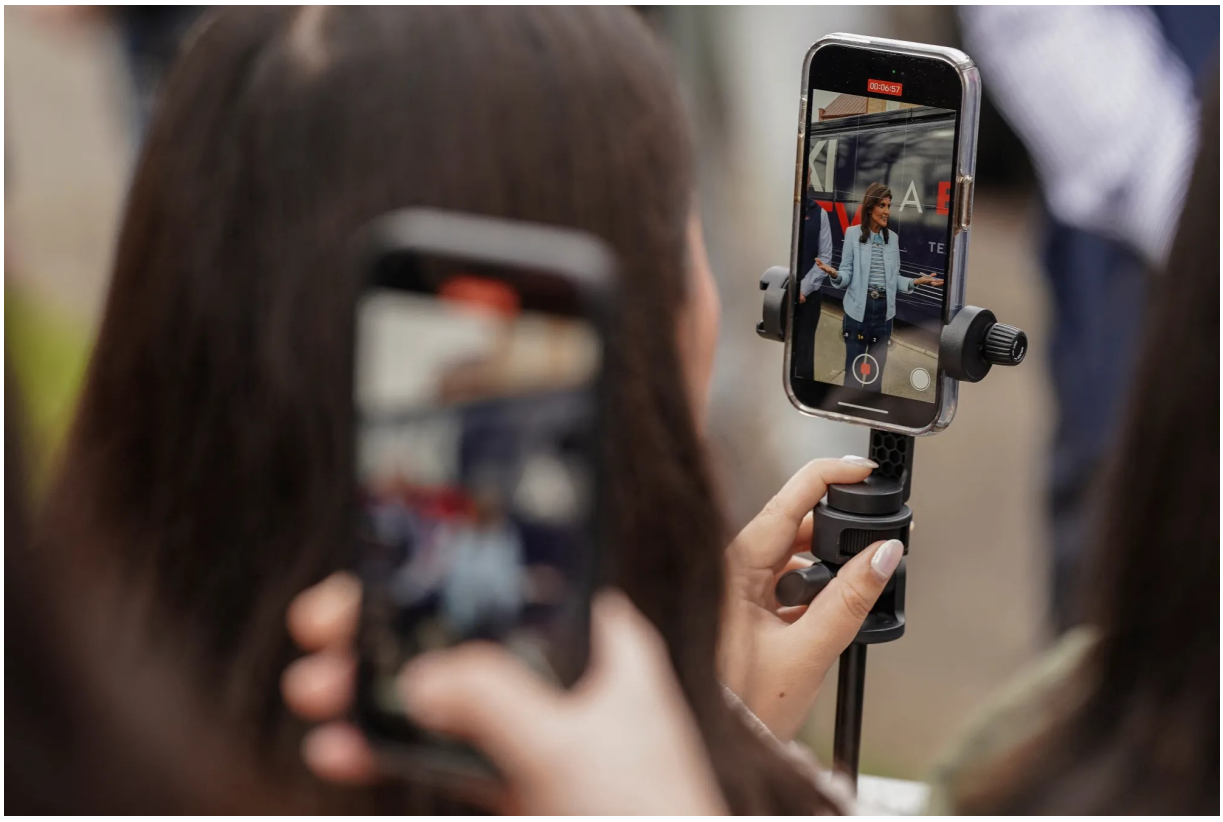
According to ACLED, extremist groups adopt hybrid tactics. It is common for groups to train for urban and rural combat with public relations and propaganda works to engage with a wider audience. Groups often place themselves in so-called "public protection" roles that increase the threat faced by journalists. Flash points for violence include swing states, state capitals, periphery towns, and rural and suburban areas.

There have been documented instances of armed extremists and militia members positioning themselves as so-called "dropbox watchers" at polling stations, with the apparent intent of intimidating and bullying both voters and poll workers.

The following should be considered for reporting from places where armed extremists may be present:

- Agree on a plan of action with your editor including indicators to withdraw.
- Plan for regular check-ins with your editor or newsroom point of contact. If working as a freelancer, consider having a check-in procedure with a fellow journalist, family, or friend.

- Avoid lone working where possible. A colleague can act as a backwatcher allowing you to focus on gathering.
- Consider your reporting location. If possible, review the location in-person or on Google Street View to identify any pinch points and avoid getting trapped in your reporting position.
- Continuously observe the atmosphere and demeanor of individuals. Pull back to a safe location when 'red flags' e.g., indicators for aggression or thrown projectiles are visible.
- Have an escape plan. Ensure that any vehicles are parked with clear exit routes.
- Consider if displaying any logos from your news outlet or press ID cards may be contentious and increase personal risk.
- Familiarize yourself with state and federal laws related to firearms possession and paramilitary activity in order to understand the types of conduct that may be unlawful.
- Refer to 'dealing with aggression' mitigations above.



Republican presidential candidate and former U.S. Ambassador to the United Nations Nikki Haley is seen on a reporter's phone as she answers a question from the media following a campaign visit in Newberry, South Carolina, on February 10, 2024. (Photo: Elijah Nouvelage / Reuters)

Committee to Protect Journalists

Digital Safety: Online harassment, disinformation campaigns and doxing

Online harassment and disinformation campaigns directed at journalists are likely to increase during the election period. Media workers face an increasingly hostile online environment exacerbated by the spread of disinformation and misinformation. They are often targeted by online attackers who want to discredit them and their work. This can often involve coordinated campaigns that leave the journalist unable to use social media, essentially forcing them offline. Protecting against online harassment is not easy, however, the more you can do to protect yourself in advance of an attack the safer you will be.

Essential steps to protect against doxing

- Regularly look yourself up online and remove personal information
- Remove personal data by signing up to services, such as DeleteMe
- Secure accounts with two-factor authentication
- Speak with family and friends about what you are happy to share and not share online
- Make a plan for what to do in case you are doxed

To minimize the risk:

Protect your personal data

- Some data is more important to protect than others. Information that can be used to locate you, contact you via a means you do not want, or can be used to confirm your identity, is best kept private where possible. This includes your home address, personal cell phone number, and data, such as your social security number or date of birth. This information is often used by online abusers to threaten journalists and also carry out identity theft.
- Check to see if your address or other personal data, such as your date of birth or telephone number, is available online. You should take steps to remove that information yourself or request for it to be removed, where possible. See CPJ's guide to removing personal data from the internet for more information.
- Sign up to have your personal information removed from data broker sites, using services such as DeleteMe, which is owned by the company Abine. Be aware that these services remove data from the most common data broker sites, so your personal information will likely continue to exist on the internet in some form. Consider signing up family members if you consider yourself at high risk of being targeted. Be mindful that it can take up to a month to have your data removed.

- Review your online profile for images and information that could be manipulated or used to discredit you. Journalists should take steps to remove any information that they feel could be used against them.
- During the election period, monitor your social media accounts for increased levels of harassment or abusive commentary.
- Be aware that there is often an uptick in online abuse during election periods. This could include targeted smear campaigns against a journalist or their media outlet.

Protect your accounts

- Protect your accounts by creating long, unique passwords for each account. Turn on two-factor authentication for all your accounts, and ideally use an app, rather than your phone number, to receive the code. Alternatively secure your accounts using a passkey. See CPJ's Digital Safety Kit to learn more about account security.
- Review the privacy settings on your social media accounts. Read more about what data is best kept private in CPJ's guide to removing personal data from the internet. Social media accounts can also reveal your location, so disable location tracking if you feel it puts you at risk.
- Turn off geo-location for posts on all accounts. If you are going to post photos showing your exact location, consider waiting until after you have left the area.
- Where possible, create professional accounts for social media.

Plan for online abuse

- If you can, speak with your newsroom or editor about any concerns you have about potential online abuse. Check if the outlet has an online abuse policy or support system for journalists who are targeted online. Editors can review CPJ's pre-assignment checklist for protecting journalists against online abuse.
- Different stories carry different online risks. Speak with your editor about possible threats and how to mitigate them, including any preventative measures you can take. Ask whether reporters who have previously worked on similar stories have received abuse online. Be aware that you are most at risk of an online attack after publishing a story.
- Know what support the newsroom can offer. For example, can they provide IT support or mental health support?
- Carry out a digital security risk assessment. Use CPJ's template to help you get started.
- Speak with family and friends about the threat of online abuse and about the type of information you do and don't want posted online. In many cases, journalists can be doxed or targeted with content posted by friends or family members.

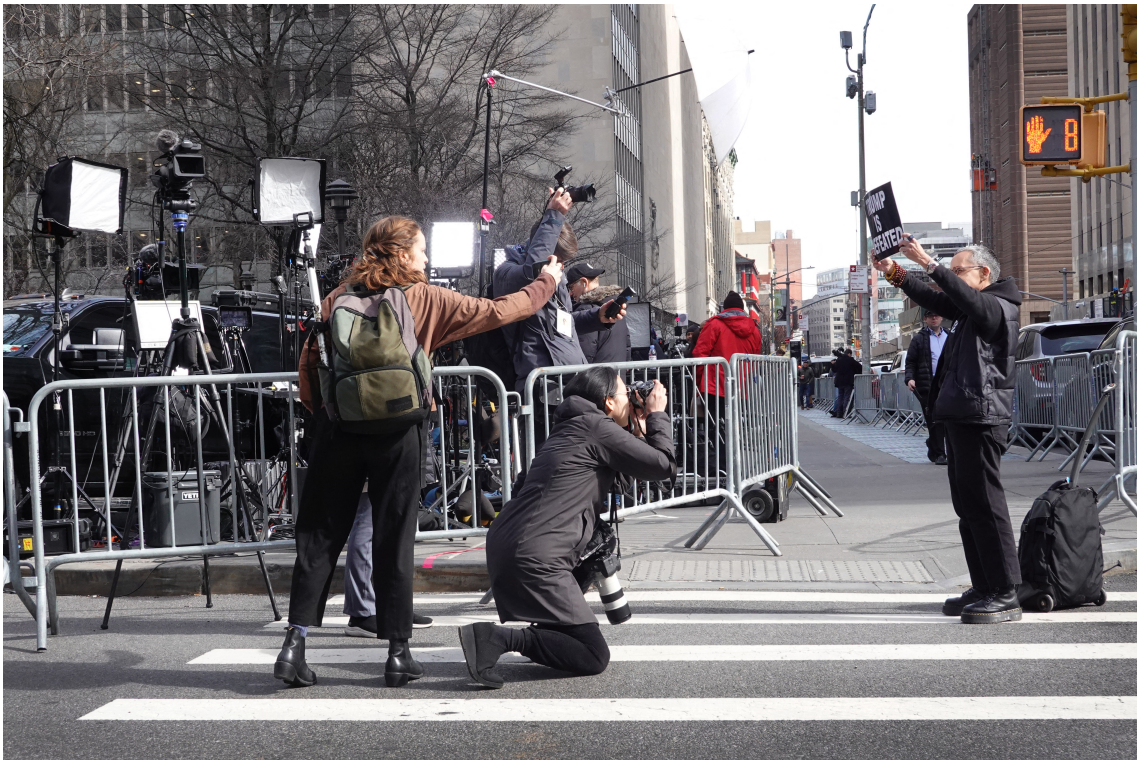
Managing online attacks

There are different types of online attacks and your response to them will likely differ depending on the threat. See the steps below for guidance.

- If personal data, such as your home address or personal cell phone number, are being circulated on the internet this means your safety is at increased risk.
- Try not to engage with those who are harassing you online, as this can make the situation worse. If you are targeted by an orchestrated smear campaign, it may be helpful to write a factual statement outlining the situation and pinning it to the top of your social media accounts. Media outlets can also write statements of support as a way to counteract a targeted campaign.
- Consider making all of your social media accounts private, and ask family members to do the same.
- Inform your family, employees, and friends that you are being harassed online. Adversaries will often contact family members and your workplace and send them information or images to damage your reputation.
- Speak with your newsroom to see what support is available to you. If you are a freelancer, or your newsroom does not have a policy in place, you can find resources at the Coalition Against Online Violence's Online Harassment Resource Hub.
- Be vigilant for any hacking attempts on your accounts and ensure that you have taken steps to update your privacy settings, set up two-factor authentication, and create long, unique passwords for each account.
- Review your social media accounts for comments that may indicate that an online threat may escalate into a physical attack. This could include people posting your address online and calling on others to attack you or increased harassment from a particular individual. Ask a trusted person to help you review your mentions or monitor your account to protect your mental health or if you are unable to monitor it yourself.
- Document any abuse that you feel is threatening. Take screenshots of the comments, including the social media handle of the person who is threatening you. This information may be useful if there is a police inquiry.
- You may want to block or mute those who are harassing you online. You should also report any abusive content to social media companies or email providers and keep a record of your contact with these companies.
- You may want to consider going offline for a period of time until the harassment has died down.

For more information and suggestions for keeping yourself safe online, consult CPJ's Resources for protecting against online abuse.

The Committee to Protect Journalists is a member of the Coalition Against Online Violence, a collection of global organizations working to find better solutions for women journalists facing online abuse, harassment and other forms of digital attack.



Journalists photograph a demonstrator protesting outside of the Criminal Courts Building as the grand jury continues to hear evidence against former President Donald Trump on March 22, 2023 in New York City. (Photo: Scott Olson / Getty Images North America / Getty Images via AFP)

Digital safety: Protecting your devices and their content

It is important to maintain best practices around securing your devices and the content contained within them. If you are detained while covering the election, your devices may be taken and searched, which could have serious consequences for both you and your sources. The police raid on the Kansas newspaper, The Marion County Record, last year, as reported by CPJ, highlights the importance for newsrooms around the secure storage of their data. The following steps can help:

Committee to Protect Journalists

Digital Safety: General best practices for election rallies and events

- Lock laptops and phones with a PIN or password. This will better protect the content on your devices if they are taken from you.
- Be aware that the authorities may be able to access your phone even if it is secured with a code. Using biometrics can be helpful if you need quick access to your phone, but journalists should be mindful that it can also give others, such as the authorities, easier access to your device. Know your rights with respect to what the authorities can and cannot do with your devices and the content stored on them.
- Update your operating system when prompted to help protect devices against the latest malware, including spyware.
- Turn on encryption for your devices if it is not already enabled by default.
- Do not leave devices unattended in public, including when charging, to avoid them being stolen or tampered with.
- Avoid using USB sticks that may be handed out at election events. These could contain malware that could infect your devices.
- Be aware that any phone conversation or SMS message sent via a cell phone provider can be intercepted, and the content obtained. To avoid this, use end-to-end encrypted messaging services, such as WhatsApp or Signal. Learn more about how to use these apps securely in CPJ's guide to encrypted communications.
- Be aware that contacts on your phone may be stored in more than one location, including in phone apps and in a cloud account linked to the phone, such as Google Drive or iCloud. Take time to review your contacts and remove anyone who could be at risk if your devices are taken and searched.
- When reporting at the event, have a process for safeguarding material that you have already collected. That way, if you are detained, the authorities will only have access to your most recent content, not all of your materials. For more information, review CPJ's guidance for journalists on the risk of arrest and detention.
- Write down on paper or your arm the contact details of key people, such as your editor or a trusted colleague, in case you are detained and your devices are taken. You may also consider writing down the number of a legal contact. The Reporters Committee for Freedom of the Press (RCFP) has a legal hotline for journalists reporting in the United States.
- Consider setting up your devices to wipe remotely. This will delete all content on your phone or laptop once activated, but only if it is connected to either WiFi or mobile data. You will need to set up remote wipe in advance, and you should give a trusted person access to the password so they can erase your content in case you are detained.

- Be aware that live streaming from an event gives away your location.
- Ideally, journalists should avoid carrying their personal phones to cover an election rally or protest. If you work for a news outlet with a budget to cover a work phone, you should request one.

Journalists who are carrying their personal phones should take the following precautions to protect their data:

- Review what information is stored on your devices, including phones and computers. Anything that puts you at risk or contains sensitive information should be backed up and deleted. You can back up your device by connecting your phone to your computer using a USB cable or in the cloud. Journalists should be aware that there are ways to recover deleted information if your devices are taken and inspected.
- When reviewing content on your phone, journalists should check information stored in apps and in the cloud.
- Think about what apps you may need on your device while covering a rally or protest. Apps for email services and social media providers contain a lot of personal information about you that the authorities or others could access if they take your phone. Think about temporarily uninstalling apps you will not need. You can install them again once you have finished covering the event.

Digital Safety: General best practice for protecting data in the newsroom

This guidance is for small- to medium-sized news outlets that may not have a dedicated IT department.

- Carry out a review of what data the newsroom has and where it is stored both physically and digitally. This could include data being stored on devices in the office, on work devices at homes of journalists, on work and personal phones and in cloud accounts and external drives.
- Know what data is essential to protect and understand what the threat could be. For example, it could be a legal subpoena, a hacking attempt, or unauthorized access being given to documents. Understanding the threat will help you decide what steps you need to take to protect the information.

- Understand the terms and services of the online services you use. Research how the company stores your data, how long they store it for, whether there have been any data breaches, and whether they have complied with legal requests for data. This will help you decide whether the newsroom should use their service or whether using it puts your data and sources at risk.

- Secure your accounts by ensuring that two-factor authentication (2FA) is turned on. Use an app, such as Authy, to receive the code and ensure that you have a copy of the backup codes for each account where 2FA is turned on. Use a password manager to generate long passwords of a minimum of 15 characters. Each account should have a different password. If you are at high risk of phishing, consider using the passkey option to secure your accounts. Encourage staff and freelancers to do the same for their personal accounts, including social media. This will help better protect accounts from hacking attempts. Read more about account security in CPJ's digital safety kit.

- Take steps to encrypt your data:

    - Turn on encryption for laptops and desktops. Use Bitlocker for Windows Pro and FireVault for Mac. You can use these programs to also encrypt external hard drives.

    - Encrypt your cloud backup using Cryptomator. You can also use Cryptomator to encrypt individual documents or folders.

    - Ensure that phones are encrypted. Android users should turn on encryption in the settings section of their device. iPhones come with encryption as standard but journalists should ensure that their cloud backup is encrypted by turning on the advanced data protection option on their devices.

- Secure all desktops, laptops and phones with a password or PIN. Be aware that law enforcement may request that you unlock them. Know your rights with regards to unlocking any devices.

- Reduce unwanted access to documents stored in the cloud by limiting access to a need to know basis and securing documents and folders with a password or PIN.

- Create a data retention policy for the newsroom detailing where data should be stored, how often data should be backed up, and how long it should be stored for.

- Have an onboarding and offboarding document that stipulates how and when access is given to accounts and ensures that access is revoked for people no longer working at the outlet.

- Know your rights should data be confiscated by the authorities.

For additional assistance, to speak directly with CPJ's Emergencies team, or enquire about safety training for you or your news organization, please email us at emergencies@cpj.org. Additional physical, digital, and mental health safety resources can be found on the CPJ Emergencies homepage.