DIGITAL SAFETY TOOLKIT

FOR YOUTH CLIMATE JUSTICE LEADERS IN SOUTHERN AFRICA

ACKNOWLEDGEMENTS

Authors: Digital Society of Africa
Published by: Project 90 by 2030
Design and Layout: Kyle Brent De Vree (devreedesign)

Contact details:
Project 90 by 2030
Address: Office 204, 16 Beach Road, Muizenberg, 7945, South Africa
Tel: +27 87 806 3501
Email: info@90by2030.org.za
Website: www.90by2030.org.za

PROJECT 90 BY 2030 Inspire. Mobilise. A low-carbon generation.

DIGITAL SOCIETY

Who is Project 90 by 2030

Project 90 by 2030 is a social and environmental justice organisation inspiring and mobilising South African society towards a sustainably developed and equitable low-carbon future.

What is the Youth Support Hub

Project 90 by 2030's Youth Support Hub is a youth-led initiative which aims to bring young people in the climate justice movement together and develop their skills, by connecting them to each other and to expert coaches who can help them grow. More information here: www.youthsupporthub.org.za

00

Why This Toolkit?

01

Understanding Digital Threats

1.1 Cyberattacks
1.2 Surveillance
1.3 Misinformation and Disinformation
1.4 Online Harassment

02

Digital Hygiene Practices

2.1 Strong Passwords
2.2 Two-Factor Authentication (2FA)
2.3 Regular Software Updates
2.4 Secure Communications

03

Data Protection

3.1 Data Encryption
3.2 Anonymity Online
3.3 Secure Storage and Backup

04

Social Media Security

4.1 Privacy Settings
4.2 Secure Posting Practices
4.3 Dealing with Trolls and Harassment

05

Emergency Response

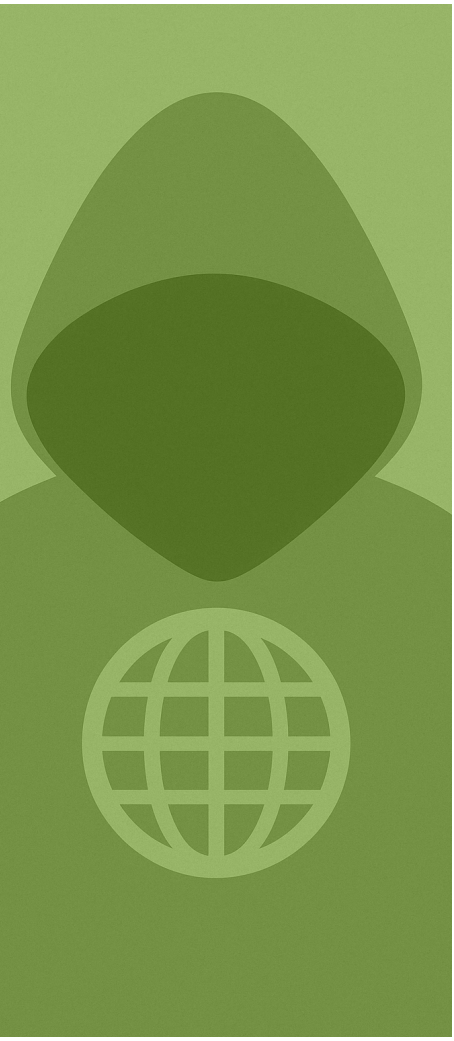
5.1 Developing a Response Plan
5.2 Support Networks

06

Toolkit Maintenance

6.1 Regular Review and Updates
6.2 Community Feedback and Improvement

TOOLKIT OUTLINE



WHY THIS TOOLKIT?

Understanding Digital Threat Faced by Climate Justice Leaders

Online action and campaigning have become essential for climate justice leaders around the globe. With the increasing reliance on digital platforms to organise, mobilise, and share information, climate change action has witnessed unprecedented growth. However, this surge in digital engagement has not come without its downsides.

Cyber-attacks, surveillance, misinformation campaigns, and online harassment are just a few examples of the challenges that have emerged. These digital threats not only endanger the personal safety of climate justice leaders, but also pose significant obstacles to the progress and impact of their campaigns. The risks that climate justice leaders face impact their work, as it detracts from their actual work and diverts time and resources towards damage control. By understanding the nature of digital threats, implementing robust security practices and preparing for potential risks, climate justice leaders can continue to advocate for climate change effectively and safely.

As the digital footprint of climate action expands, so too do the risks and threats that climate justice leaders face, compromising their safety and the effectiveness of their efforts.

Some of the effects of digital and cyber threats on youth climate justice leaders include:

1. Surveillance causes climate justice leaders to engage in self-censorship for fear of harm that may befall them or their families. This takes away from the main message.
2. Hate speech causes psychological harm and diverts from their main work. Climate justice leaders spend more time in self-defense than on their actual work. Hate speech in some cases ends up delegitimizing their work and as such more time is spent on sharing the same messages instead of working on new projects.
3. Disinformation makes it difficult for climate justice leaders to effectively campaign as the public has a prejudiced perception of them and their work. It has also been seen that audiences are more receptive of messages based on the image they have of the ‘messenger’.

01

UNDERSTANDING DIGITAL THREATS

1.1 Cyberattacks

**Malicious actions taken by criminals and other individuals to disrupt, compromise or damage electronics, computer systems or networks. These attacks can target different aspects of computer networks, digital infrastructure, hardware and software.*

Common Types of Cyberattacks:

- **Distributed Denial of Service (DDoS)** - aimed at disrupting normal platform functioning through overwhelming a system, network or website with traffic, making it temporarily or permanently unavailable. Such an attack may lead to financial loss, reputation loss, website unavailability and service disruption.
- **Malware** – shortened from 'malicious software' – it can take on many forms that can compromise computer systems, networks or users. Malware can steal sensitive information, gain unauthorized access to information or even cause damage to certain data. The various forms of malware include:

i. **Viruses –** malicious code that attach to files or programs, executing when opened and causing file deletion or corruption.

ii. **Worms –** unlike viruses, these are standalone programs that replicate and spread independently. Worms take advantage of vulnerabilities in a network, and use this to spread to other computers.

iii. **Trojan horse -** this is a type of malicious software that disguises itself as a legitimate and safe program, but contains malicious code. Once it has gained access to the system, it can create back-doors for attackers, install spy-ware or steal sensitive data among other things.

iv. **Ransomware -** this is software that encrypts your files or computer, making them inaccessible. The attacker demands a ransom, often in cryptocurrency, in exchange for the decryption key.

v. **Spyware -** just as the name suggests, this type of malware is primarily used to spy on the user. It takes note of browsing habits, location services, key strokes and other sensitive information.

Who can be targeted by cyberattacks?

With action online, social media platforms of climate justice leaders tend to be at risk of different cyber-attacks – in particular harvesting of sensitive information and phishing attacks. Websites are also often a sweet spot for attackers, vulnerabilities in your website can lead to loss of service and/or reputation as well as theft of important information.

1.2 Surveillance

**The systematic monitoring of individuals, groups or activities to get information, influence behavior or gain and maintain control. There are several types and methods for surveillance:*

Electronic Surveillance

- **Closed Circuit Television Surveillance –** CCTV used to track the movements of a person of interest in specific areas.
- **Audio Surveillance –** conversations or phone calls monitored and recorded using microphones or other audio devices

Communication channel surveillance – tracking of electronic communications, such as emails, browsing habits and computer usage.

Social Media Surveillance - Monitoring and tracking of social media platforms to get information about the user. This can be done manually or using automated systems.

Surveillance indicators

Phone Surveillance	Email Surveillance
At least two or more of these factors have to be true before one can reasonably begin to suspect that their mobile device is under surveillance:	
Battery drains faster than usual, while not in significant use and the phone is of reasonable age. This may indicate the presence of malicious background processes.	**Frequent attempts at account log-ins** from an unfamiliar location could be a sign that your email is compromised.
Unexplained and excessive mobile data usage could indicate that there is an application using your data possible to export files.	**Unusual password change requests** often signify that someone is trying to gain access to your email.
Excessive heat from the phone may indicate that there are several background processes running.	**Strange email forwarding or filtering rules** indicate possible compromise, it is important to be aware of what rules you have in place for your inbox.

Phone Surveillance	Email Surveillance
At least two or more of these factors have to be true before one can reasonably begin to suspect that their mobile device is under surveillance:	
Delayed shutdown or restart could be as a result of surveillance software running in the background.	**Unfamiliar emails in your outbox or sent box** may indicate that someone is sending and receiving emails on your behalf. This may also be true for emails that you did not open suddenly being marked as read.
Strange pop-ups or messages are usually an indication that your phone is compromised.	
Unusual apps with excessive permissions could be surveillance software.	

Who could be watching?

Despite there being a continued need for climate action, oftentimes, climate justice leaders are labeled as criminal groups and are suppressed from protesting by governments. Groups under surveillance are often monitored through their emails, phone conversations and GPS locations. However, governments and prosecuting authorities are not the only entities engaging in surveillance. Fossil fuel companies often spy on climate justice leaders and their activities, sometimes keeping track of them for years.

1.3 Misinformation and Disinformation

**Misinformation refers to the spread of false information, either by mistake or with the deliberate intent to mislead. When false information is spread with the deliberate intent to mislead audiences, it is called disinformation.*

Recognizing Disinformation

How do we recognize disinformation?

Disinformation is not just spread at random. It is often a targeted effort to compromise and weaken the credibility of groups. According to a 2018 research study conducted by MIT Scientists, **'fake news'** spreads six times faster than factual information. People who spread disinformation often use different tactics to spread their messages faster.

This checklist may be useful for determining whether information found online is authentic:

- **Does it elicit strong emotions in you?**

  Manipulated information often plays on the emotions of audiences. Think carefully about why this information appeals to your emotions or those of your audiences.

- **Is the source of information clear?**

  If the information can be clearly traced back to a credible source, it is more than likely to be accurate. False information often has no clear or traceable sources.

- **Does the website or person sending the information seem credible?**

  While it is possible to pose as a credible news outlet, there are ways to tell if someone or a publication are credible. If it's on social media, you can check to see when the page was created. On Twitter/X, you can check if the page is verified and affiliated to a more credible organization. On Facebook you can check if they are verified. If it is a website, you can check for small giveaways such as poor grammar, no real sources, use of stock images. You can alsocheck when the website was established, by using tools like Wayback Machine, which can show when a website was established among other tools.

- **Does the information seem fair and balanced?**

  Often, websites and social media posts sending out false information do not stop to consider journalistic practices of balance and fairness. Indeed purveyors of false information often use sensationalist language, and pay little to no attention to spelling and grammar mistakes. The stories are often not logical (as they are counting on audiences to react to headlines).

- **Does it check out with other publications?**

  If a story is true and of significance, there will usually be other reputable sites that carry the story. This is also helpful to cross examine stories and fill in details that one publication or post may have deliberately left out.

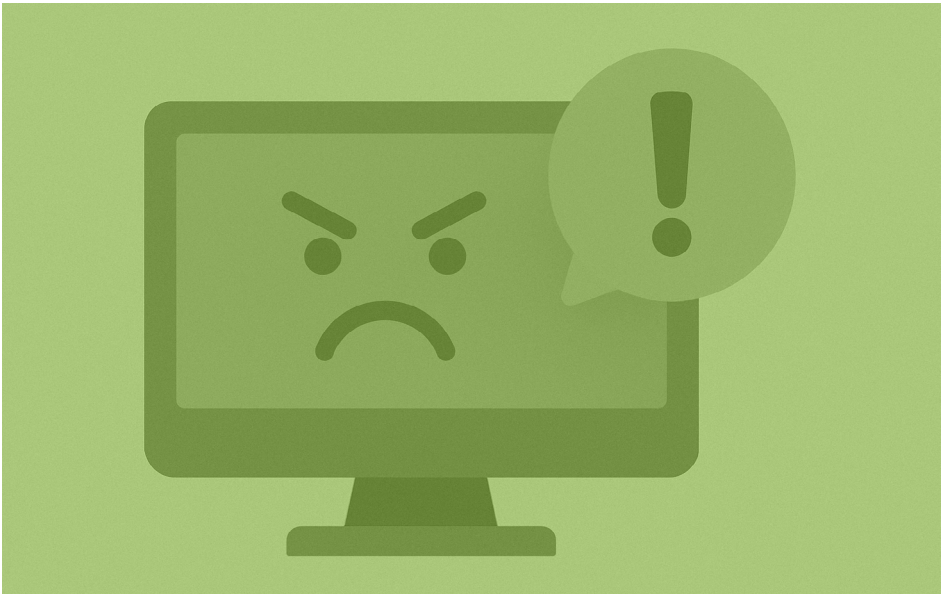
Countering Disinformation

But how do I counter disinformation?

- Understand disinformation and how to recognize it
- Use your platforms wisely to build your own credibility.
- Understand the motives of those spreading disinformation and see how you can counter it.
- Be very careful with what information you share and amplify and ensure that you have done as much fact checking as possible before sharing anything
- Set the facts straight by maximizing access to correct and factual information
- Invest in media literacy and this can be done by educating people on climate change, with verifiable information.

1.4 Online Harassment

Online harassment includes stalking, cyber-mobbing, unsolicited messages, and cyber-bullying based on factors like appearance, intelligence, or gender, etc. Doxxing, where personal information is shared without consent, is another form of harassment, often aimed at causing offline harm. Blocking and reporting are effective ways to stop this, but documenting instances (e.g., through screenshots) is crucial if pursuing legal action. It's important to know your legal rights and what constitutes prosecutable behavior.



DIGITAL HYGIENE PRACTICES

2.1 Strong Passwords & Password Management

Passwords are your information's first line of defence. Common mistakes often include using easy to guess passwords or same passwords across multiple platforms.

So, when creating strong passwords you should consider URL:

- **U**nique: avoid password reuse across multiple accounts
- **R**andom: letter combinations that don't spell a word, so that it cannot be guested by brute force or data dictionary attacks eg: k7T` D1+r&o_uWJ8
- **L**ong – Think a minimum of 12 characters or more, or even better a phrase rather than a word.

Password Managers

Remembering our long and unique passwords can be difficult so using a Password Manager is a good solution. This is a database that stores and remembers all your passwords for you, all you need is to remember the Master password; so don't forget it or you may lose access to the rest of your passwords. There are many options but for climate justice leaders – offline, free and open sources options like KeePassXC are recommended. Whilst a good online app is Bitwarden.

2.2 Two-Factor Authentication

Two-factor authentication (2FA) is an essential security measure that adds an extra layer of protection to your online accounts beyond just a password. 2FA significantly reduces the risk of unauthorized access.

- The first factor is your password or PIN, which is something you know.
- The second factor being something you have, it could be a mobile device that receives a unique code via **Implementation of 2FA.**

To implement 2FA:

- First, enable the feature in the security settings of your online account.
- Secondly, choose a second verification method, such as receiving a code via SMS, using an authenticator app (i.e Google Authenticator, Authy and Microsoft Authenticator), or a physical security key.
- Thirdly, follow the setup instructions provided.

Once activated, you'll need both your password and the second factor to access your account, significantly enhancing its security.

2.3 Regular Software Updates

Keeping software and our devices like smart-phones, tablets and computers updated is essential. These updates ensure that fixes for security, latest operating systems, and firmware updates are installed. Making sure that our digital health is up-to-date ensures that we significantly reduce our risk of security breaches, malicious attacks, and overall improves our devices performance.

Check whether your device is up to date by going to the device settings and check search for pending updates. However, best practice is to set to automatically perform updates and receive the latest security patches and improvements as soon as they are available. This is crucial for maintaining strong security, as it minimizes the window of opportunity for hackers to exploit known vulnerabilities.

2.4 Secure Communications Encrypted Messaging Apps

End-to-end encryption in messaging apps means that your data is encrypted while in transit. This means that it cannot be read until it reaches the intended recipient's device.

Signal is a recommended secure messaging app, known for not collecting any personal information or other information about users, except your phone number which is used to register.

Wire secure communication platform offering end-to-end encryption for messages, voice and video calls, and file sharing. It features strong privacy policies, an open-source protocol, and supports multiple devices per account for seamless synchronization. Favored by climate justice leaders, journalists, and organisations, it emphasizes privacy and security. A unique aspect is that it doesn't require a phone number for registration.

Email Services

Proton Mail

Proton Mail is a secure email service that provides end-to-end encryption,the message body and attachments are all encrypted. If you are using Proton Mail with your recipient, the emails are encrypted by default, however, if your recipient is not a ProtonMail user, the email will be encrypted in transit, meaning that the email service provider may be able to read your messages.

Alternatively, you may use PGP for encryption, which works with a pair of keys, one public and one private. The email is encrypted using a private key, and can only be decrypted when the recipient uses the public key you provided them with.

Tutanota Mail

Tutanota is a secure email service that offers end-to-end encryption, ensuring that only the sender and receiver can access the content of the emails. With a strong focus on privacy and data security, Tutanota also includes features like encrypted contacts and calendars, making it an all-encompassing secure communication solution. Its user-friendly interface and commitment to not tracking users' data make it a suitable choice for climate justice leaders who prioritize confidentiality and security in their digital communications.

DATA PROTECTION

3.1 Data Encryption

Full & Partial Disk Encryption

Climate justice leaders should consider using full or partial disk encryption for protecting the sensitive data residing on their devices.

- Full disk encryption (FDE) secures all data on a disk drive, ensuring that every file, system data, and even the operating system itself, are encrypted. This means if the device is lost or stolen, the data remains inaccessible without an encryption key.
- Partial disk encryption, on the other hand, allows users to selectively encrypt only certain files or folders, offering flexibility but potentially leaving unselected areas vulnerable to unauthorized access.

Both methods significantly enhance data security, but the choice between them should be based on the user's specific needs and the sensitivity of the data being protected. Be sure to remember your password and recovery key for the encryption, if you don't the device cannot be decrypted and the information will be lost for good. On Windows, you can enable full disk encryption on Bitlocker and on MacOS, the encryption service is FileVault. These however have their own limitations which include requiring certain hardware platforms in order to work correctly. A recommended free and open source multi-platform software that provides free disk encryption is Veracrypt.

3.2 Anonymity Online

Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) are essential tools for enhancing online privacy and security. VPNs create a secure, encrypted tunnel between a user's device and the internet, hiding the user's IP address and safeguarding data from eavesdroppers, especially on unsecured public Wi-Fi networks. By routing the user's internet connection through a server in a different location, VPNs also allow for the bypassing of geo-restrictions and censorship, providing access to a broader range of information and resources. However, it's vital to choose a reputable VPN provider, as the VPN service has access to all transmitted data. A trustworthy VPN should maintain a strict no-logs policy, ensuring that users' activities are not recorded, thereby upholding the principles of anonymity and privacy crucial for climate justice leaders, journalists, and anyone concerned about their online security.

TOR Browser

The Onion Router (TOR) routes user' internet traffic through a global network of volunteer-run servers, significantly obscuring the user's location and usage from anyone conducting network surveillance or traffic analysis. This makes it an essential tool for climate justice leaders, journalists, and individuals in repressive regimes, providing a safer way to access the internet without revealing their identity or location. The TOR Browser is designed to access the deep web and is particularly effective in bypassing censorship, allowing users to access information and communicate securely. However, while TOR greatly enhances privacy, it can also lead to slower internet speeds due to its complex routing system. Users should also be aware of the security settings and best practices while using TOR to ensure maximum protection and effectiveness. One should be wary about unwittingly sharing identifiable information even while using TOR. It is also important to note that some countries criminalize the use of TOR and other circumvention techniques.

3.3 Secure Storage and Backup Best practices

Taking care of your digital security is really important, especially when it comes to protecting sensitive information. Using encrypted cloud services lets you access your data from anywhere while keeping it safe, even when it's being sent or stored online. External drives with encryption also help protect your data, especially if the drive gets lost or stolen. It's also super important to back up your data regularly, so if anything goes wrong, you can recover your important information. These steps help keep your data safe and private, which is especially important for climate justice leaders.

Backup Strategies

Some back up strategies include:

- Scheduling regular and automated backups.
- Having multiple backup options – which guards against a single point failure. If one back up fails, you have other options. The 3-2-1 back-up strategy is recommended for this.
- Documentation and procedures – your back up plan should include procedures handling information, clarity on what gets backed-up, secure deletion if needed and relevant user privileges.

SOCIAL MEDIA SAFETY

4.1 Privacy Settings

For climate justice leaders operating online, managing social media privacy settings is vital for security, limiting visibility, contact, and location to reduce the risk of surveillance and harassment.

Climate justice leaders should regularly review and update these settings to counteract changes in social media platforms' policies and functionalities. Additionally, being cautious about the amount and type of personal information shared on these platforms can prevent potential threats from exploiting this data. Utilizing features like profile locking, where available, and segmenting contacts into different lists for varying levels of information access can further enhance privacy. Ultimately, these practices help maintain a safer online environment, allowing climate justice leaders to continue their important work while reducing their vulnerability to digital threats.

4.2 Secure Posting Practices

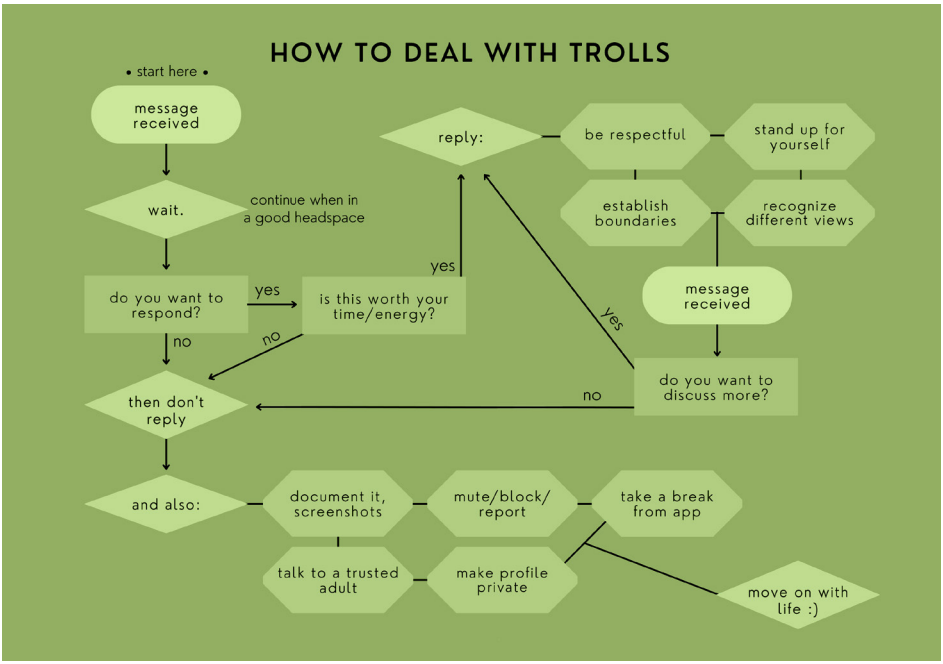
There is a temptation to use social media as an online diary, especially if you feel you are speaking to a void. However, it is important to be very careful and selective about what information you share:

- Limit posting personal information (e.g., full names, IDs, phone numbers) to avoid impersonation or phishing.
- Protect the privacy of close friends and family by avoiding photos or details, especially of children or relatives.
- Customize the audience for your posts and be cautious about who can view them.
- Be wary of friends or follow requests, especially from strangers, and avoid accepting them unless you know the person.
- Consider creating a separate page for networking or community building, managed by multiple people.

4.3 Dealing with Trolls and Harassment

Oftentimes, there will be people online who will attack you and your ideas. Sometimes it is a coordinated attack to discredit you and the work that you do, other times people use anonymity to be abusive. This may not only create negativity but also distract from the main purpose of your online advocacy. Some best practices when facing trolling and online harassment include:

- Don't feed the trolls. Sometimes responding directly fuels trolls, and may embolden them to attempt to humble you online. Usually ignoring and muting them works, and it may be useful to block repeat offenders.
- Document instances of abuse, especially if they are threatening to harm you. If you are able to and have gathered enough evidence, you may take this to the police for further action.
- Report abusive users to the platform. If they have clearly abrogated platform guidelines, their accounts may be suspended or permanently banned.
- Understand platform rules, if only so that you yourself use the platform responsibly, and your reports are accurate and effectively summarize the offense.
- Schedule digital detoxes. Operating in a toxic online environment can have serious real-life mental health consequences, and may contribute to depression and anxiety. Taking a digital detox and connecting with a supportive community can help ease the stress of being online.



EMERGENCY RESPONSE

5.1 Developing a Response Plan:

As the case of Greta Thunberg, a Swedish climate justice leader known for raising public awareness of climate change across the world amongst young people, has shown, prominent climate justice leaders can be the targets of scathing attacks on social media that range from trolling to death threats. It is crucial for climate justice leaders to have a clear and actionable strategy as well as immediate steps and actions to take in case of a digital and physical attack or threat:

- **Identification:** Quickly determine the nature and extent of the attack. Understanding what has been compromised (e.g., accounts, devices, networks) is crucial for an effective response.
- **Containment:** Immediately take steps to limit the spread or impact of the attack. This may involve disconnecting affected devices from the internet, changing passwords, or isolating compromised areas of a network.
- **Assessment:** Evaluate the severity and potential consequences of the attack. This helps in prioritizing response efforts and determining the necessary resources for addressing the issue.
- **Notification:** Inform relevant parties about the breach. This could include team members, a legal adviser, or, in severe cases, law enforcement. Transparency with affected parties can be crucial, depending on the nature of the data or systems compromised.
- **Recovery:** Work on restoring and securing your digital environments. This includes cleaning infected systems, recovering lost data from backups, and patching vulnerabilities to prevent future attacks.
- **Review and Learn:** After addressing the immediate threats, review the incident to understand how it happened and how it was handled. Use this analysis to strengthen your security measures and response plans for future incidents.

By having a response plan that includes these elements, climate justice leaders can ensure a swift and organized reaction to digital threats, minimizing damage and recovering more effectively

Climate Justice Leaders Safety Measures

a. **Secure Sensitive Materials:** Store all sensitive documents and equipment securely when not in use. Maintain an updated inventory list to quickly identify if anything is missing or compromised, particularly in the event of a break-in or raid.

b. **Preparedness for Raids or Searches:** Organize your space so that sensitive documents and equipment are secure and can be quickly concealed or moved if necessary. Understand your legal rights concerning raids and searches.

c. **Emergency Planning:** Ensure that you have a well mapped and documented emergency plan. This should include things like code words and who to contact if things go wrong.

d. **Training and Drills:** Conduct regular security training and emergency drills for all members of your team. Being prepared and knowing how to respond can significantly reduce risks and improve safety during unexpected situations.

5.2 Support Networks:

Creating and leveraging community support networks is an essential strategy for climate justice leaders, particularly in emergency situations. This section outlines how to build and utilize these networks effectively:

a. **Identify Allies:** Find local climate justice leader groups, organizations, legal aid, and individuals who share your goals or can provide support in times of need.

b. **Build Relationships:** Establish and maintain regular communication with these allies. Attend community meetings, participate in local events, and support other groups' initiatives to build goodwill and mutual support.

c. **Develop Communication Channels:** Set up secure and reliable communication channels for coordinating with your network. This can include encrypted messaging apps, email lists or phone trees. Ensure that all members know how to use these tools effectively and understand operational security measures.

d. **Share Resources and Information:** Pool resources like legal advice, tech support, and medical help to strengthen the community's emergency response.

e. **Coordinate Training and Workshops:** Organize or participate in training sessions and workshops on relevant topics such as legal rights, first aid, digital security, and emergency response. Knowledge is a crucial asset in crisis situations.

f. **Establish Emergency Protocols:** Develop clear protocols for different types of emergencies, such as legal troubles, cyberattacks, or physical threats. Make sure these protocols are understood and accessible to all network members.

g. **Regular Updates and Check-Ins:** Maintain regular check-ins within your network to update on current threats, share best practices, and provide mutual support. Regular communication helps in building trust and ensuring that the network remains active and responsive.

h. **Leveraging 'green influencers'** and people less exposed to risk i.e international organizations – to advocate on their behalf. Using influential climate justice leaders and international organizations can be a good way to amplify advocacy and reach a wider audience.

TOOLKIT MAINTENANCE

Maintaining the relevance and effectiveness of the digital safety toolkit is essential for ensuring the continued safety and efficacy of climate justice leaders' work. This section outlines key practices for toolkit maintenance:

6.1 Regular Review and Updates:

- **Stay Informed:** Keep abreast of evolving digital threats by regularly consulting trusted cybersecurity sources and networks. The landscape of digital security is constantly changing, and new threats can emerge swiftly.
- **Adaptation:** Assess and adapt to new threats by updating the toolkit's recommended tools, practices, and strategies accordingly. This may involve introducing new software, updating security protocols, or revising response strategies.
- **Regular Audits:** Conduct regular audits of the toolkit to ensure all components are up to date and functioning as intended. This includes reviewing the effectiveness of security measures and the relevance of guidance provided.
- **Update Schedule:** Establish a regular schedule for reviewing and updating the toolkit. This could be semi-annually, annually, or more frequently if significant changes in the digital threat landscape occur.

6.2 Community Feedback and Improvement:

- **Feedback Mechanism:** Create a mechanism for receiving feedback from users of the toolkit. This could be through online surveys, email feedback, or community forums. Open channels for feedback encourage community participation and ownership.
- **Engagement:** Actively engage with the wider climate justice leader community to share knowledge, updates, and experiences related to digital security. This can include hosting workshops, participating in forums, or collaborating with other organizations.
- **Incorporate Feedback:** Regularly review feedback received from the community and incorporate relevant suggestions into the toolkit. This iterative process ensures the toolkit remains responsive to the needs of its users.
- **Sharing Best Practices:** Foster an environment of learning and improvement by sharing updates, new best practices, and success stories within the community. This not only enhances the toolkit but also builds a stronger, more informed climate justice leader network.