10,000 cases

STRENGTHENING CIVIL SOCIETY'S DEFENSES

WHAT ACCESS NOW'S DIGITAL SECURITY HELPLINE HAS LEARNED FROM ITS FIRST 10,000 CASES

DIGITAL SECURITY HELPLINE
accessnow

accessnow.org/help

accessnow

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

DIGITAL SECURITY HELPLINE

accessnow

Access Now's Digital Security Helpline is a **free-of-charge** resource for civil society around the world. We offer **real-time, direct technical assistance** and advice to civil society groups and activists, media organizations, journalists and bloggers, and human rights defenders. Our **24/7** services are available with support in **nine languages**: English, Spanish, French, German, Portuguese, Russian, Tagalog, Arabic, and Italian. We respond to all requests within two hours.

A Note on our data

This report looks at cases Helpline managed since 2013. Over the years, the Helpline continued to improve the way we categorize cases we receive with learnings from our experience in supporting the global community. In 2016, we adjusted the methodology to catalogue our cases in order to bring clarity and visibility of our work and the challenges our global communities are facing. Through the research for this report, we revisited and cleaned our data to ensure the analysis is a true reflection of the state of the civil society Helpline supports.

While we try to be comprehensive, our data spans almost a decade and relies on the specific context of each specific case. The technical and operational constraints mean that the numbers in our documentation may evolve with further refinement of our methodology and documentation. If you would like to make further inquiries, please contact us as help@accessnow.org.

Photo credits: Victoria Heath, Hassen Selmi, and o10.tn

June 7 2021

This paper is an Access Now publication. It is written by Daniel Bedoya, Michael Carbone, and Sage Cheng. We would like to thank the Access Now team members who provided support, including Gustaf Björksten, Natalia Krapiva, Rogelio López, Beatrice Martini, Peter Micek, Melody Patry, Hassen Selmi, Brett Solomon, Carolyn Tackett, and Donna Wentworth, and all the members of the Access Now Digital Security Helpline who have made this work possible.

We would like to acknowledge the role of our CTO Gustaf Björksten who conceptualized the Helpline in the early years, and has worked tirelessly for over a decade, together with the Helpline Director Daniel Bedoya, to bring it to life. Additionally, all of the Helpline staff, from Tunisia to Costa Rica to the Philippines and beyond, who have responded heroically day and night to clients in distress, deserve our deepest gratitude.

We would also like to thank the global community of civil society help desks for their ongoing collaboration and support. The Helpline has and remains a free-of-charge resource for civil society around the world because of the tranformational support the transformational support of SIDA, the Swedish International Development Cooperation Agency, whose confidence in the Helpline enabled this service to grow from a concept to a living program.

We are also indebted to a portfolio of other donors who have provided crucial, ongoing support to the Helpline, including the Dutch Ministry of Foreign Affairs, Facebook, the Ford Foundation, the German Federal Foreign Office, Global Affairs Canada, Google, Luminate Group, Microsoft, the Mott Foundation, Twitter, and the Wellspring Philanthropic Fund. Our funding policy can be found here: https://www.accessnow.org/financials.

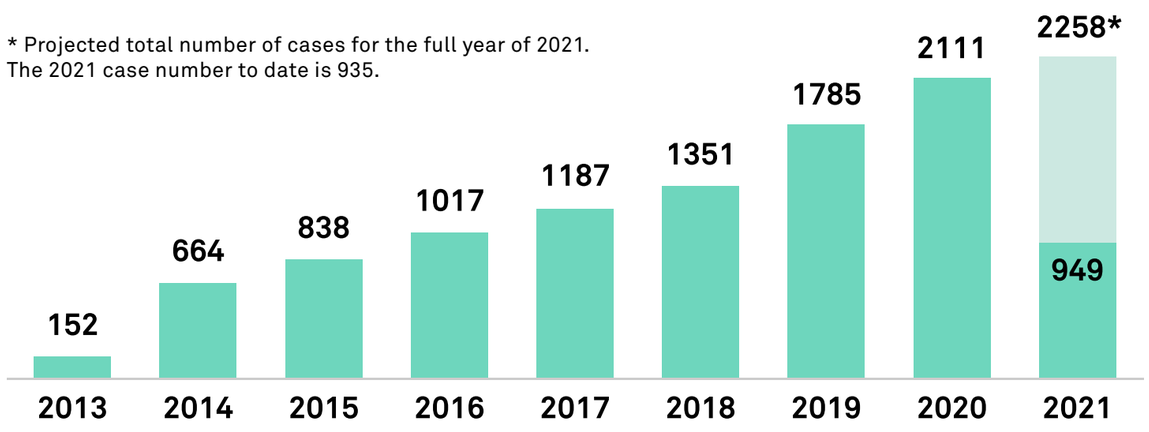
We look forward to receiving feedback on these findings and working together to continue developing new ways to strengthen digital security for human rights defenders around the world.

TABLE OF CONTENTS

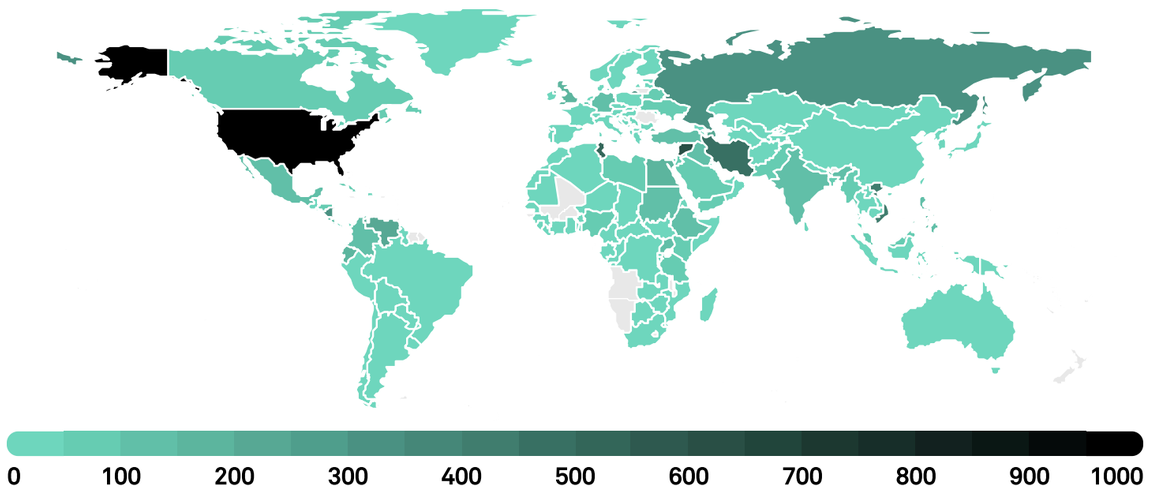
AN OVERVIEW OF THE FIRST 10,000 HELPLINE CASES

Number of Helpline cases started per year (2013-2021)

* Projected total number of cases for the full year of 2021.
The 2021 case number to date is 935.



Regional distribution of Helpline cases (2013-2020)



Middle East & North Africa: 25.8%

Latin America & the Caribbean: 15.9%

Asia Pacific: 15.3%

Europe: 14.2%

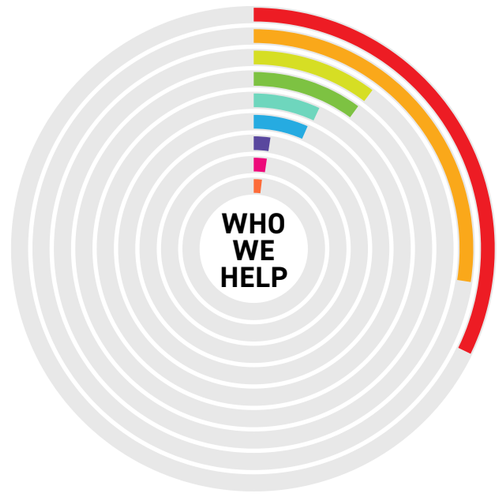
North America: 11.0%

Africa: 9.1%

Global: 4.6%

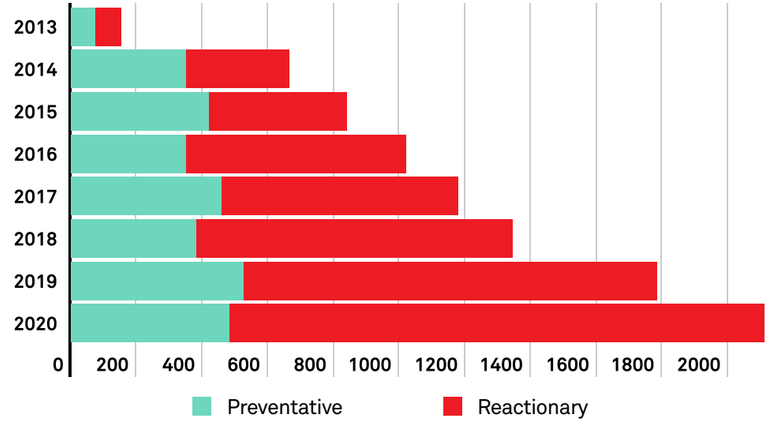
Unknown: 4.1%

Who has received support from the Helpline (2013-2020)



- NGO / Non-Profit / Collective: 32.2%
- Human Rights Activist: 27.4%
- Independent Media: 10.2%
- Unknown: 10.1%
- Other: 6.9%
- Journalist: 6.6%
- Human Rights Lawyer: 2.4%
- Blogger: 2.3%
- Academia / Researchers: 1.9%

Number of preventative cases vs. reactionary cases by year (2013 -2020)



Trending threats targeting civil society

- → Account compromise
- → Malware
- → Censorship
- → Denial of Service and other website attacks
- → Harassment
- → Communications surveillance

What we learned

- → Digital attacks are shrinking civil space
- → Companies controlling the infrastructure we depend on are leaving us in the dark
- → Civil society continues to be severely under-resourced and under capacity
- → It takes our entire trusted network to achieve our mission
- → The ecosystem of support for civil society must keep growing
- → Tailored support achieves the greatest impact
- → Diversity makes us stronger
- → Investing in self-care makes our work more sustainable

ABOUT THE ACCESS NOW DIGITAL SECURITY HELPLINE

Providing digital security advice and support to at-risk users has been a core pillar of Access Now's work since the early days of the organization, more than 10 years ago. During the 2009 Iranian election, millions came together both in person and online to organize, protest election fraud, and report on human rights abuses, despite the government blocking internet access, censoring content, and undermining its opponents' online security. Access Now began as an emergency response team of technologists working to help people get back online, broadcast citizen media to the world, and ensure their safe communications.

From there, the organization invested progressively in creating what is now known as the Digital Security Helpline, which documented its first case in our distributed ticketing system on August 23, 2013. Seven years and a few months later, the team received its 10,000th request for assistance. As we reach this important milestone, we would like to share with our community some reflections on what we have observed, what we have learned, and where we are heading.

The Digital Security Helpline is a 24/7 computer security incident response team (CSIRT) that provides assistance to at-risk groups and individuals from civil society, including activists, journalists, and non-profit organizations.[1] We are the first civil society-focused CSIRT to have been accepted as a full member of the Forum of Incident Response and Security Teams (FIRST), the premier global forum of such organizations.[2]

After four years of informally supporting civil society beneficiaries across the world, the Helpline was formally established in 2013, with an initial team in Tunisia. Shortly after, team members in Costa Rica and the Philippines completed the base structure that has enabled the team to provide 24/7/365 support — without interruption — since May 2014. If you want to get more familiar with the work of the Access Now Digital Security Helpline, we encourage you to have a quick look at our website and the list of services we provide.[3] And if you need help, please do not hesitate to contact us at help@accessnow.org.

As we reflect on receiving 10,000 requests for assistance, it is worth emphasizing that each case represents an individual story, often involving someone risking their life to defend their human rights or those of others. Therefore, this milestone is a bittersweet achievement, and rather than celebrating it we take it as an opportunity to reflect on the threats faced by civil society around the world, as seen through the Helpline's daily work.

[1] Access Now Digital Security Helpline. https://accessnow.org/help.
[2] Daniel Bedoya and Edward Herbert. A world FIRST: Access Now Digital Security Helpline brings civil society focus to leading global incident response network. June 6, 2019. https://www.accessnow.org/first-digital-security-helpline/; FIRST. https://www.first.org.
[3] Access Now Digital Security Helpline. https://accessnow.org/help; Digital Security Helpline Services. https://www.accessnow.org/helpline-services/.

We wouldn't be here without our partners

Since the beginning of the Helpline, we have worked alongside other organizations to respond to urgent incidents and to provide longer-term assistance to civil society around the world.

The Helpline is a proud founding member of CiviCERT, a network of Computer Emergency Response Teams (CERTs), Rapid Response teams, and independent Internet Content and Service Providers focusing on supporting civil society to prevent and address digital security issues.[4]

The Helpline regularly coordinates with trusted partners, including CiviCERT members, as well as other digital security help desks, civil society organizations, and tech companies, to resolve or consult on cases.

As an example of the importance of the Helpline partners in our work, over the course of 2020 we handled 2,111 cases, of which:

41.0%

were received by the Helpline from other partner organizations

20.9%

were referred by the Helpline to trusted partners

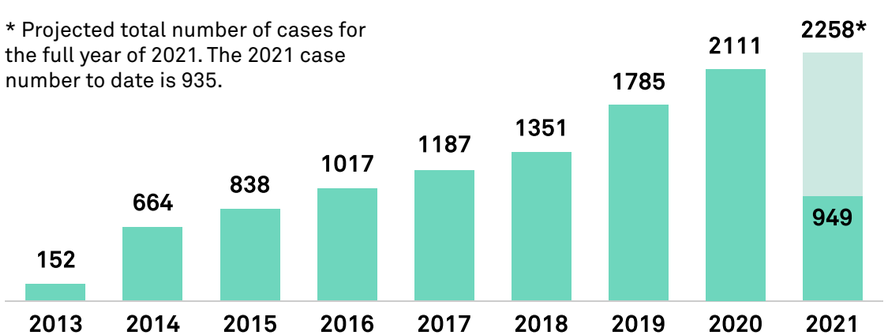
We are honored by the trust placed in us to do this work, and try to make sure we meet the needs and expectations of our partners to defend and extend the rights of at-risk users around the world.

Reaching 10,000 requests

Since we received the first case in August 2013, the number of requests for assistance has grown consistently year over year. Figure 1 shows the number of cases we have managed yearly since the beginning of the Helpline's operations. In nearly eight years, we have grown from receiving 152 requests per year to 2,111, representing 1,288.8% growth in the number of cases.

Figure 1. Number of Helpline cases started per year (2013-2021)

* Projected total number of cases for the full year of 2021. The 2021 case number to date is 935.



[4] CiviCERT: Computer Incident Response Center for Civil Society. https://civicert.org.

We have been able to scale up the support we provide with modest staffing increases over the years by creating clear processes and workflows for common cases, and by growing and supporting the ecosystem of regional and local help desks. We share these workflows publicly for feedback and to support other help desks and jumpstart their work.

Documentation

The Helpline is continuously growing its library of documentation to store our collective knowledge, improve the quality of our services, and contribute to the global community of other help desks. We maintain various public documentation such as:

- **Community Documentation:** These topic-based articles and email templates are the foundation of the Helpline's work. They capture our collective knowledge on different digital security topics, and currently include over 150 articles across 20 categories and over 120 email templates across 11 categories.[5]
- **User Guides:** These are thematic hands-on guides for individuals to navigate through digital safety issues, such as email encryption, travel safety, anti-doxxing, and online dating safety.[6]
- **A First Look at Digital Security:** This interactive visualization provides an introduction to assessing risks.[7]
- **Digital First Aid Kit:** This collaborative CiviCERT initiative helps civil society actors connect with the digital security team best suited to assist their specific needs or emergency.[8]

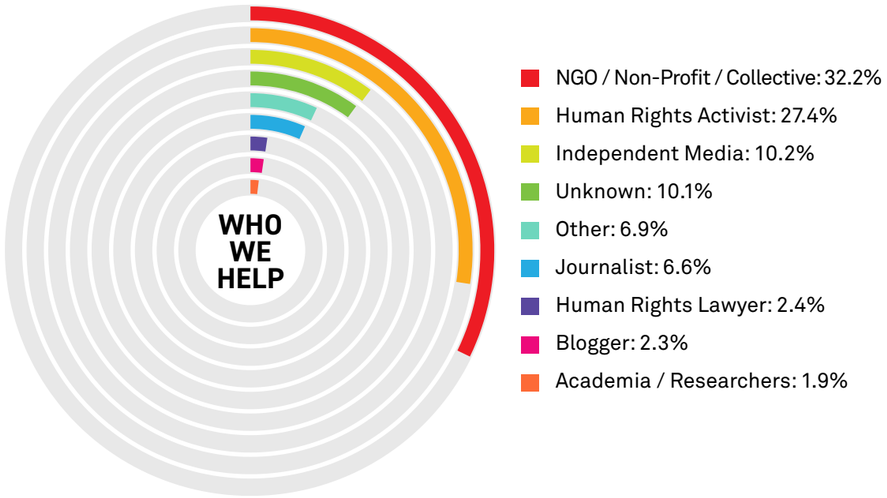
All of the resources above are also available on GitLab to facilitate community re-use, feedback, and collaboration.[9]

Who we help

Our work spans civil society from individual activists, human rights defenders, and members of marginalized communities, to media workers — including bloggers, journalists, and independent media — and larger organizations and institutions.

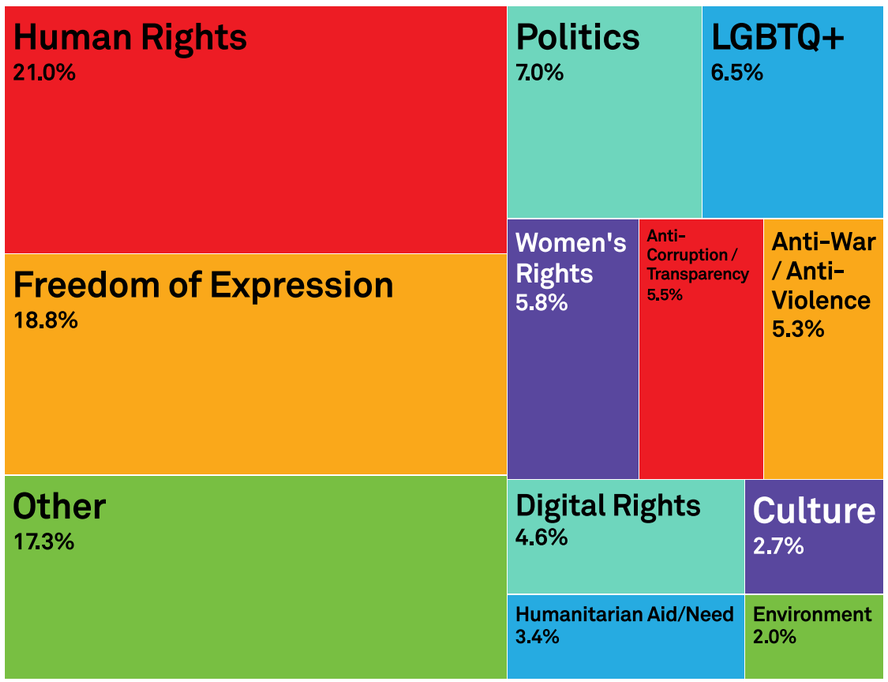
[5] Digital Security Helpline Community Documentation. https://communitydocs.accessnow.org.
[6] Access Now Helpline Guides. https://guides.accessnow.org.
[7] Sage Cheng and Kim Burton. Don't Panic! Download "A First Look at Digital Security." Updated October 2020. https://www.accessnow.org/first-look-at-digital-security/.
[8] CiviCERT. Digital First Aid Kit. https://digitalfirstaid.org.
[9] GitLab. Access Now Helpline. https://gitlab.com/AccessNowHelpline.

Figure 2.Helpline beneficiaries by type (2013-2020)



Helpline beneficiaries engage in a diverse range of activities in the defense of fundamental rights, addressing the many unique challenges of at-risk individuals and communities around the world. Figure 3 presents the most common areas of focus of the Helpline's beneficiaries.

Figure 3. Helpline beneficiaries by area of focus (2013-2020)

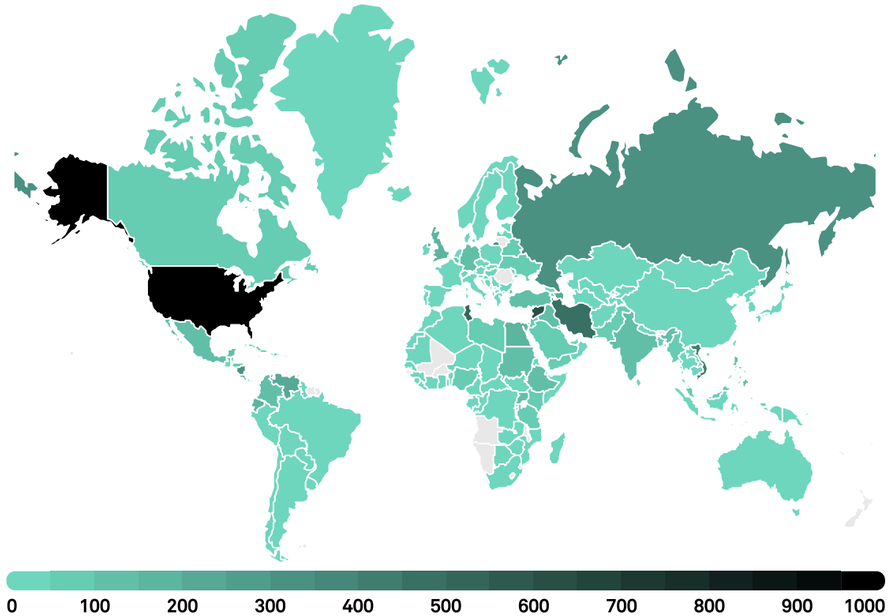


Where we work

The Helpline's mandate is global, and we have supported individuals, groups, and organizations from 161 different countries around the world. The most active regions and countries have shifted over time due both to the growth of the Helpline's network of partners and intermediaries as well as in response to shifts in social and political contexts.

Figure 4 shows a heat map of what have been the most active regions and countries in the cases managed by the Helpline between 2013 and 2020. As the map illustrates, there are only a limited number of countries that have not seen civil society assisted by the Helpline.

Figure 4. Helpline cases by location (2013-2020)



To support this global work, we have a global team, based in Tunisia, Costa Rica, the Philippines, Germany, and remotely, to allow us to be available 24/7/365.

Multilingual

The Helpline currently provides support in nine different languages. The language we most frequently used to manage cases was **English**, followed by **Spanish**, **Arabic**, **French**, and **Russian**. 29.6% of the requests we received were at least partially managed in a language other than English.

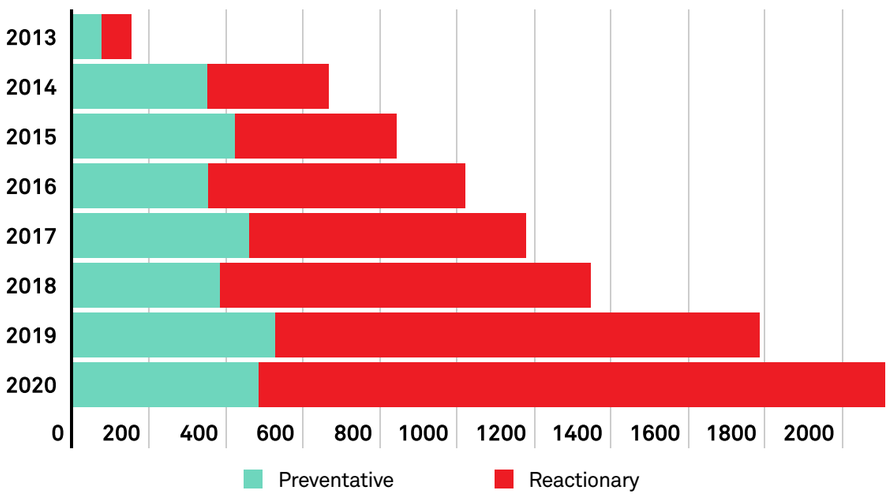
EXPLORING OUR FIRST 10,000 CASES

At this point in the growth of the Digital Security Helpline, we are taking a step back to reflect on some of the key trends and findings that have emerged from our work so far. We recognize the cases we've worked on and the organizations, groups, and individuals we work with are not a scientific sample of civil society, but rather reflect the unique relationships we have built over the Helpline's existence. We are proud to share what is currently one of the most comprehensive views available of digital threats to civil society around the world. We look forward to discussing the trends and needs further as a team and in close collaboration with our partners in the space.

Urgent incidents and preemptive assistance

Within those 10,000 requests for support, there are cases that run the gamut from urgent emergency assistance to long-term organizational security support. We use the term "reactionary" to refer to those situations where an incident is already taking place and the support is oriented toward management and recovery, and use "preventative" to describe cases that are initiated before incidents occur to preemptively improve the online safety of the beneficiary. **Out of the cases between 2013 and 2020, the majority (66.7%) have been us reacting to urgent incidents.**

Figure 5. Annual number of preventative and reactionary cases (2013-2020)



As seen in Figure 5, up until 2015 the numbers of preventative and reactionary cases were comparable. Starting in 2016, the Helpline observed a sustained growth in the number of reactionary cases, resulting in a larger difference in preventative vs. reactionary cases every year. For example, in 2020, three out of every four cases received by the Helpline were reactionary.

On average, it took four and a half weeks to complete a Helpline request

Preventative cases took longer on average — six weeks — while the average time for resolving reactionary cases was around four weeks. Our team's capacity has expanded and efficiency improved since 2013, and our response times have consistently shortened as a result.

This difference highlights a couple of changes to the Helpline and our work over the years. As our internal processes and documentation have expanded and stabilized, it has enabled us to process more urgent cases, as our responses often need to follow particular steps.

In addition, political conflicts and unstable environments often led to additional urgent requests, and our work in these contexts has only increased over time. We observed that groups working in **civil and political rights, activists and organizations in conflict zones, political activists, and individuals and organizations with a focus on freedom of expressio**n were more likely to reach out for help with pressing security incidents than for preventative support.

Surges of Helpline cases in conflict zones

A full 92.9% of the 640 cases relating to Syria and 84.8% of the 92 cases relating to Libya dealt with emergency incidents. Requests for support in Myanmar surged 500% at the start of the military coup, and we received our highest number of requests relating to Ukraine in 2014 during the Euromaidan revolution.

The highest number of cases we received in one 24-hour period was on June 4, 2019, relating to Sudan, with 24 cases in relation to the violent repression of protesters and associated network shutdown. The Helpline works closely with the #KeepItOn coalition to fight against network disruptions and shutdowns around the world.[10]

We did not see an increase in the raw number of preventative cases, but there **has been a significant evolution in how the Helpline manages this preventative and educational work.**

We have moved from a more isolated approach to support to an approach characterized by a holistic assessment of the security of groups and organizations, often undertaken over a longer period of time and in collaboration with partners. We have integrated more professional methodologies for security assessments such as the SAFETAG framework into our work, improving our internal skills and processes, and ultimately providing better results to the groups we work with.[11]

The following table demonstrates this shift by presenting the top preventative categories we have observed every year since 2013.

[10] #KeepItOn: Fighting internet shutdowns around the world. https://www.accessnow.org/keepiton.
[11] SAFETAG. https://safetag.org.

Table 1. Top preventative case categories (2013-2020)

Note: The Helpline adjusted its methodology for categorizing cases in 2016.

2020	2019
No.1 Security assessment No.2 Online account security No.3 (tie) Email security No.3 (tie) Device security	No.1 Online account security No.2 Security assessment No.3 Website protection
2018	**2017**
No.1 Online account security No.2 Email security No.3 Security assessment	No.1 Email security No.2 Security assessment No.3 Website protection
2016	**2015**
No.1 Email security No.2 Security assessment No.3 Website protection	No.1 Email security No.2 Host, data security No.3 Secure text chat
2014	**2013**
No.1 Email security No.2 Denial of Service protection No.3 Host, data security	No.1 Email security No.2 Secure browsing

We can see the ascension of security assessments to becoming the most common preventative case category in 2020. In practice, this shift means that **although the number of preventative cases the Helpline team handled has not increased each year, we have significantly extended the time and effort we are able to put into each case.** Here is one testimonial from a Helpline beneficiary that illustrates what this process can entail:

> Thanks to the incredible input of Access Now we have gained so much knowledge about protecting ourselves against attacks on our digital security and communications infrastructure. This is of particular importance given the increasing repression against actors working within our field.
>
> Access Now has drawn up an extensive security policy that is specifically adjusted to our structure. We received advice on specific queries regarding our phone system, VoIP-services, and the local contexts of our activists. Due to the support provided by the Helpline, we have changed the tools we're operating with, adopted encryption, and revised the manner with which we create passwords (just to name a few), and have thus raised our overall level of security. Access Now has gone through every step of our operations, sensitizing us to risks and providing solutions to eliminate them. Access Now's input has created a much higher level of awareness about the importance of securing our communications.
>
> Furthermore, Access Now assisted us with the actual implementation of more secure apps, tools, and services — offering to provide local trainings to ensure everybody is able to use and understand these necessary services. Generally, the Helpline has been extraordinarily proactive, flexible, reliable, and engaged. Our whole network is deeply grateful for their work.
>
> We look forward to further collaboration and are completely supportive and convinced of the aim and cause of Access Now's work. Thank you so much. We would be in a catastrophic security situation without you.

The Helpline during the COVID-19 pandemic

Unsurprisingly, our team members also handled cases **relating both directly and indirectly to the COVID-19 pandemic**. In a relatively small number of these cases in 2020, Helpline beneficiaries themselves directly attributed their digital security request to the pandemic, but the true number of cases related to COVID-19 is almost certainly far higher. Of the cases specifically identified as related:

- About 19.4% of those asking for help sought support with video conferencing (VoIP platforms);
- Four cases related to censorship in the context of COVID-19, involving either the abuse of content-flagging features to restrict access to information, or blocked access to health information due to government restrictions/disinformation;
- Numerous beneficiaries sought assistance with storing data or sharing sensitive information; and
- Several cases were reactionary in nature, involving defense and mitigation of phishing and malware attacks that leveraged COVID-19 as a contextual frame for the attack/scam.

Beyond the cases beneficiaries identified as COVID-related, there were also 20 unique requests for VoIP support — a significant increase from six such cases in 2018, and four in 2019.

Trending threats targeting civil society

With the majority of Helpline cases responding to urgent incidents, we have seen many civil society actors operating in unique contexts around the world face similar threats. There are also several types of attack that may be less frequent but are extremely dangerous in their impact. We explore several of these trending threats below.

Table 2. Top categories of reactionary cases (2013-2020)

Note: The Helpline adjusted its methodology for categorizing cases in 2016.

2020	2019
No.1 Account compromise No.2 Censorship No.3 Harassment	No.1 Account compromise No.2 Censorship No.3 Harassment
2018	**2017**
No.1 Account compromise No.2 Censorship No.3 Harassment	No.1 Account compromise No.2 Censorship No.3 (tie) Harassment No. 3 (tie) Phishing / suspicious messages

2016	2015
No.1 Account compromise	No.1 Account recovery
No.2 Censorship	No.2 Account protection
No.3 Phishing / suspicious messages	No.3 Malware
2014	**2013**
No.1 Account recovery	No.1 Account recovery
No.2 Censorship	No.2 Website Denial of Service
No.3 Website Denial of Service	No.3 Censorship

1. Attacks from all sides

Throughout this report we make reference to "attackers" and their tactics for targeting civil society organizations. But to understand the full scope of the problem, we must understand not only the tactics but also who is behind them.

Attribution remains one of the biggest challenges in the digital security space — especially for civil society, whose resources to defend against attacks are already limited, let alone adequate to conduct the complex forensic analysis necessary to determine who is behind an attack. Access Now's Digital Security Helpline is continuing to develop its capacity in this area, and we work closely with partners like Citizen Lab[12] to facilitate its research on landmark cases.

What is clear from observation, though, is that civil society is facing increasingly sophisticated attacks from all sides. For example:

- Governments around the world are investing in their capacity to silence dissent, whether it be through tools for both mass and targeted surveillance, equipment to censor and implement internet shutdowns, or entire agencies dedicated to manipulating content moderation policies on social media platforms.
- Companies that develop censorship and surveillance equipment have flagrantly refused to adopt meaningful human rights policies or due diligence that would prevent such tools from getting into the hands of governments or other actors who intend to abuse them.
- Targets of advocacy efforts, such as private sector actors and others who find themselves on the receiving end of civil society's demands, also often use aggressive opposition research tactics to silence them, including harassment, reputational attacks, and smear campaigns.
- For women, LGBTQ+ folks, people of color, indigenous groups, religious minorities, and others who experience discrimination and marginalization in their everyday life, some members of the **general public** may pose a threat. When **law enforcement, political figures, or religious and other community leaders** signal it is appropriate or even encouraged to target certain people with hate and violence, many individuals will follow.

It is also important to note that digital threats often lead to or intersect with physical dangers as well, and it is our top priority to help ensure civil society actors everywhere can stay safe while also effectively carrying out their work. To that end, we work closely with other help desks that specialize in legal assistance, psychological support, and other services essential for our beneficiaries' resilience and well-being, and we aim to strengthen this network going forward.

[12] The Citizen Lab. https://citizenlab.ca.

2. Account compromise

Among the urgent cases we received since 2014, it is **account recovery cases** — where a person has lost control of or access to an online account, like their email or social media profile — that are consistently the most common. [13] In 2020 alone, the Helpline managed 487 requests associated with compromised accounts.

In the vast majority of account compromise incidents we handled, beneficiaries were using third-party infrastructure over which they did not have direct control. This creates additional challenges, since recovery of the account often requires coordination with and support from the third-party platforms in question.

The Helpline's experience working with these service providers is decidedly mixed. Some providers neglect to offer any type of support at all, while others — though providing support in some cases — far too often fail to devote the staff time or resources necessary to help their most vulnerable users swiftly mitigate attacks or effectively prevent future account compromise. While Access Now is appreciative of the support provided by the Trust and Safety teams at many of these companies, it is not enough. We have consistently raised the alarm — both to the tech sector writ large and directly to individual companies — about the emerging human rights crisis on their platforms, as well as the significant gap between what is needed to address it and what they have been willing to invest.

Figure 6. Helpline cases involving account compromise on common platforms (2016-2020)

[13] Initially, the "account recovery" category of cases included situations where an account was compromised, the user was locked out, or the account was inaccessible for unknown reasons, including because an online platform banned the account. In 2016, we adjusted the methodology for case categorization to provide greater visibility and understanding of the work we conduct, and this recategorization included cases dealing with issues regarding online accounts.

In addition, attackers have developed increasingly sophisticated tactics to overcome common strategies for protecting accounts.[14] For example, we've seen attackers:

- impersonate social media support teams to steal credentials or to get official documents from victims that can then be used to claim their accounts;
- use the promise of two-factor authentication — an important tool for protecting account access — in "social engineering" attacks designed to trick users into handing over password reset codes; and
- set recovery methods within the compromised account to help them retain access even after control of the account is "restored" to the rightful owner.

What you can do

- Enabling two-factor authentication remains a very important step to protect control of your accounts.[15]
- In many cases where we helped recover an account, the recovery information was not available or current, greatly complicating the recovery process. Check your recovery information — such as your recovery email account or phone number — to be sure it is up to date!

> Access Now is the most important help resource for activists in the region, their rapid response has allowed us to ensure the safety and secure the information of important activists in our organization. They have helped mediating with social media platforms with regards to impersonation cases and reports of fake news. Without the help from Access Now, many young activists from our country would be in a greater state of vulnerability, these activists have been targets of online attacks on their social media profiles and thanks to the support of the Helpline, the theft of sensitive information was avoided.

In a reflection of the growing importance of having a social media presence, since 2018 we have seen increased demand for assistance in preventing compromise of online accounts before it happens, and it is now among the most frequent preventative requests. This increase in requests for assistance preventing these kinds of attacks came a slow five years after requests for assistance recovering from them topped our list of reactionary cases (see Table 2). At the Helpline, we hope to work with help desks globally to vastly reduce the time between recognizing a security crisis for civil society and working aggressively to put in place proactive measures to prevent harm.

3. Malware

There are trending threats that are important even if there are not a large number of cases in the category. While malware cases only broke the top three on the list of reactionary case types in 2015, and the related cases of phishing and suspicious messages only reached the top

[14] See, for example, Access Now Helpline Team. The "Doubleswitch" social media attack: a threat to advocates in Venezuela and worldwide. June 9, 2017. https://www.accessnow.org/doubleswitch-attack/; Access Now Helpline Team and Carolyn Tackett. New Facebook phishing attack taking Vietnamese opposition voices offline. October 22, 2018. https://www.accessnow.org/vietnam-facebook-phishing-attack-take-opposition-voices-offline/.
[15] Nathan White. Decoding two-factor authentication: which solution is right for you? September 14, 2017. https://www.accessnow.org/decoding-two-factor-authentication-solution-right/.

three in 2016 and 2017, these cases are often connected to the most serious abuses of human rights perpetrated in the digital space, with severe consequences for the victims and society at large. This was demonstrated in 2018 when attackers used NSO Group's "Pegasus" malware to target associates of Saudi journalist and human rights advocate Jamal Khashoggi. It is likely the attack facilitated the surveillance and information gathering necessary for his murder by the Saudi regime.[16]

While attackers can use suspicious messages and phishing attempts to compromise online accounts, they can also leverage these tactics to plant malware that compromises the security of an entire device. This can enable the attacker to get all sorts of information about the victim, such as their private messages, confidential documents, or the online accounts they access on the device. The attacker can also leverage what they find to gain access to other kinds of sensitive information, such as data on a human rights organization's networks and infrastructure.

Over the years, we have received and investigated reports of more than 161 potential malware attacks. **Among our Helpline beneficiaries, the people most likely to be targeted for malware attacks were journalists and independent media, followed by NGOs working to defend human rights.** The actors who target these groups often use off-the-shelf surveillance technology, and the Helpline team works with other parts of Access Now to hold the companies that make these products accountable for facilitating human rights violations. [17] Many of the countries where victims are targeted — such as Mexico, Saudia Arabia, and Turkey — have been the site of surveillance and spyware campaigns linked to state actors.[18]

4. Censorship

Another common type of incident reported to the Helpline and reflected in Table 2 is online censorship. Although the Helpline has supported organizations trying to circumvent blocking of websites they manage or the hosting providers or other infrastructure they use, the vast majority of cases we handle regard censorship on social media platforms. These individuals and organizations often report attackers manipulating a platform's reporting mechanisms or abusing legal avenues, such as copyright complaints, to get their content taken down. There are currently only limited mechanisms to protect people from these types of attacks or mitigate the damage, reflecting the unfortunate reality that many of these **platforms lack the necessary mechanisms and/or capacity to ensure people get fair remediation**. Attackers can make disingenuous copyright-related claims and get content taken down during critical social and political moments when people need to see it most, so that even when the content is later restored, the attacker has still "won" the news cycle by blocking the target's content.[19]

[16] Access Now. Two years after Khashoggi's slaying, no accountability for spyware firm or Saudi government. October 1, 2020. https://www.accessnow.org/khashoggi-two-years-later/; Citizen Lab. The NSO Connection to Jamal Khashoggi. October 24, 2018. https://citizenlab.ca/2018/10/the-nso-connection-to-jamal-khashoggi/.
[17] *See, e.g.,* Access Now. Access Now tells the 9th Circuit Court: NSO Group cannot escape accountability in U.S. courts. December 23, 2020. https://www.accessnow.org/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/; Natalia Krapiva and Peter Micek. Francisco Partners-owned Sandvine profits from shutdowns and oppression in Belarus. September 3, 2020. https://www.accessnow.org/francisco-partners-owned-sandvine-profits-from-shutdowns-and-oppression-in-belarus/.
[18] *See* Javier Pallero. International groups reject Mexican government surveillance of public health advocates. February 16, 2017. https://www.accessnow.org/international-groups-reject-mexican-government-surveillance-public-health-advocates/; Access Now. Two years after Khashoggi's slaying, no accountability for spyware firm or Saudi government. October 1, 2020. https://www.accessnow.org/khashoggi-two-years-later/; Access Now. European-made FinSpy malware is being used to target critics in Turkey. May 14, 2018. https://www.accessnow.org/european-made-finspy-malware-is-being-used-to-target-activists/.
[19] We provide further details on the Helpline's approach to censorship cases in these posts: Daniel Bedoya and Natalia Krapiva. Digital Security Helpline: our approach to content-related cases. May 12, 2020. https://www.accessnow.org/digital-security-helpline-our-approach-to-content-related-cases/; Natalia Krapiva, Rodrigo Rodriguez, and Alejandro Menjivar. Warning: repressive regimes are using DMCA takedown demands to censor activists. October 22, 2020. https://www.accessnow.org/dmca-takedown-demands-censor-activists/.

5. Denial of Service and other website attacks

In Table 2, we can also see the story of denial of service (DoS) attacks against civil society websites. The number of such attacks reported by organizations we helped peaked in 2017, and has since gradually declined. However, other civil society data sources and security industry reports all show both the number and scale of DoS attacks designed to block civil society online content has continued to increase. We see **the decrease in cases we received as a reflection that providers of DoS protection services**, both from civil society — like Deflect and Qurium — and the private sector — like Project Galileo,[20] **are mitigating many of these attacks.**

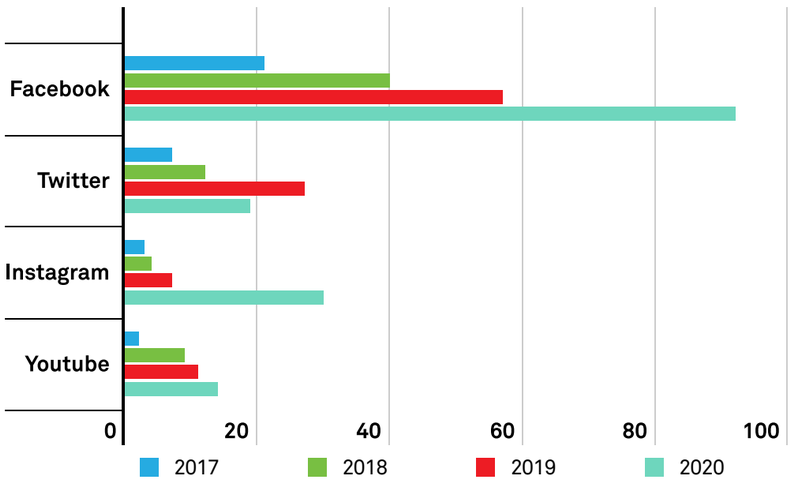
Beyond responding to DoS attacks, we broadly support both reactive and preventative cases to harden civil society website security. This is a critically important service, as civil society relies on their websites to engage and share their work on their own terms.

6. Harassment

Another type of case that has only increased since 2017, as reflected in Table 2, is online harassment, and specifically harassment of women and members of the LGBTQ+ community using social media platforms. In 2020, Helpline beneficiaries reported 180 incidents, a whopping 56.5% increase over the previous year, relative to an 18.3% increase in total cases in the same period.

This dangerous trend has been reported widely, and through the Helpline, we have observed its devastating impact first hand.[21] Harassment is often intertwined with attacks on a target's online accounts. Among our Helpline beneficiaries working to defend women's rights, the most frequent type of attack they reported involved both online harassment and the compromise of online accounts. During the COVID-19 outbreak, we have seen national lockdowns to limit the spread of the disease lead to aggressive targeting and harassment of LGBTQ+ communities.[22]

Figure 7. Helpline cases involving harassment on common platforms (2017-2020)



[20] Deflect: Get protected. Stay connected. https://deflect.ca; Qurium: The Media Foundation. https://www.qurium.org; Cloudflare. Project Galileo. https://www.cloudflare.com/galileo/.
[21] *See* Pew Research Center. The State of Online Harassment. January 13, 2021. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/; PEN America. No Excuse for Abuse. https://pen.org/report/no-excuse-for-abuse/.
[22] Sage Cheng and Gustaf Björksten. Digital Security Helpline: In 2020, LGBTQ groups are facing more online harassment than ever. June 29, 2020. https://www.accessnow.org/digital-security-helpline-in-2020-lgbtq-groups-are-facing-more-online-harassment-than-ever/.

> The Digital Security Helpline is really useful for us as an NGO and for our queer community. Indeed we receive several requests for help from people who have been hacked, harassed and who are in the process of being blackmailed and each time the Helpline helps us enormously with the necessary expertise to overcome the problem.
>
> In addition, the Helpline also intervenes to help our staff, when we face a technical problem, with their depth of knowledge to find solutions. We really appreciate your help and support, and we respect the serious and wonderful work you are doing.

7. Communications surveillance

Whether it is journalists protecting their sources, lawyers protecting their clients, human rights defenders collecting evidence of abuses, or activists holding the powerful to account, most of the people our Helpline serves are facing threats of communications surveillance from their adversaries. Implementing secure channels of communication is one of the first lines of defense in keeping civil society safe and empowered to do its work. It is also one of the first steps in the Helpline's support process for beneficiaries, so people can openly share with us their needs, issues, and concerns in a trusted environment.

Cases involving **email security** have consistently remained a top category for us since we started the Helpline, with the exception of 2019, as seen in Table 2. This indicates that email remains an important shared communications channel. The Helpline itself, as well as our partners and beneficiaries, rely on it as a free, federated communications medium in our daily work.

However, keeping email secure — such as by ensuring our email messages are end-to-end encrypted — is a burdensome experience, and the process is not mobile-friendly. Because of this, **many folks prefer to use secure-by-default messaging apps** such as Signal,[23] and the Helpline is exploring ways to allow us to better integrate messaging apps like Signal into our day-to-day work.

A snapshot: our 10,000th case

An attacker used a Facebook account to impersonate Facebook staff, creating a page designed to look like an official Facebook company page. The attacker then tagged a Costa Rican women's rights NGO on Facebook claiming they had been reported to the platform. The post displayed a message instructing the NGO to resolve the complaint by logging in to confirm its account, using a link that redirected to a fake login page hosted outside Facebook. Fortunately, the targeted organization did not click on the phishing link and instead shared the post and link with the Helpline. Together, we were able to get both the false Facebook page and the phishing website taken down.

The Helpline then shared information about the phishing site within the CiviCERT community to warn other civil society organizations and prevent them from getting targeted. We also uploaded the phishing URL to Google Safe Browsing and Netcraft,[24] which makes it so that browsers and antivirus tools automatically identify a site as malicious. This protected others from attacks while we worked to get the Facebook page and phishing site removed.

Across Latin America and the world, women's rights groups face attacks online, not just from governments and institutions, but also within societies.

[23] Signal. https://signal.org.
[24] Google Safe Browsing. https://safebrowsing.google.com; Netcraft. https://www.netcraft.com.

Women are often targets of harassment, doxxing, censorship, and other forms of gender-based violence online. Organizations and groups working to defend women's rights face additional challenges. Not only are they working to protect women, they are also working to protect themselves from the same kind of violence.

Out of all cases the Helpline has handled related to women's rights organizations, 63% were reactionary, with the largest number of cases (23.6%) related to account compromise, followed by harassment (9.4%) and censorship (7.6%). Facebook was the platform where Helpline beneficiaries reported the most attacks (20.5% of cases), followed by Twitter (10.3%) and Instagram (8.9%). These findings provide evidence to show that women's rights organizations (and women in general) continue to be disproportionately targeted for attack on social media platforms.

WHAT WE LEARNED

A few of the lessons we have learned from almost eight years of operation and 10,000 cases include:

→ Digital attacks are shrinking civic space

We had hoped that as awareness of digital attacks and potential digital safety measures increased, we would see a shift from reactionary to preventative cases. However, we saw the opposite, and in 2020, we handled more urgent incidents than ever before. It appears that preventative security measures have not kept pace with the significant increase in online attacks against civil society actors, and our experience at the Digital Security Helpline points to a global shrinking of safe online space for civil society.

→ Companies controlling the infrastructure we depend on are leaving us in the dark

The vast majority of the urgent incidents the Digital Security Helpline has observed are taking place on infrastructure that is not controlled by civil society. This reduces the visibility of potential threats and forces both the at-risk user and the Helpline to depend on a third-party company to cooperate in tackling the incident. It appears that most corporate infrastructure and service providers do not yet fully understand the real impact of their decisions on the most vulnerable people using their services. Their response to attacks on civil society — when they have a response — is often lacking and systemic problems are not adequately addressed. Wherever possible, we encourage civil society and the communities they serve to explore free, open-source tools and platforms that give you more control over your information.

→ Civil society continues to be severely under-resourced and under capacity

From our security assessments with civil society groups, we see a need for civil society to strengthen its baseline security practices, particularly given attacks it faces from extremely well-resourced adversaries. This disparity of resources between target and attacker has no equal elsewhere in digital security. Civil society groups need dedicated and sustainable resources to build a foundation of basic security practices, as well as in-house expertise, to carry out their work safely.

→ It takes our entire trusted network to achieve our mission

In the last few years, almost half of all cases the Helpline received have been referrals from our trusted networks and partners, such as CiviCERT. As a global team supporting individuals from everywhere in the world, we recognize there are limitations to our support and reach, and we firmly believe that a strong, well-resourced, diverse, trust-based ecosystem of support is the only way to protect vulnerable users against the growing number of threats.

→ The ecosystem of support for civil society must keep growing

We publicly share the documentation and workflows we use on the Helpline so that other help desks can use them, and so others can give us feedback to improve these resources together.[25] We actively work to expand the membership of CiviCERT to build more resilient regional help desks and ultimately a more resilient global support ecosystem.

→ Tailored support achieves the greatest impact

Each person who reaches out to the Helpline — whether looking for individual or organizational support — works in an environment with unique risks, threats, and needs. Our strength is being able to engage individually and tailor the support we provide to their experience, context, and needs to ensure the most sustained positive impact.

→ Diversity makes us stronger

Just as a diverse and inclusive ecosystem is necessary to create a resilient support system for global civil society, a diverse, multifaceted, multicultural Helpline team is of utmost importance to provide effective assistance. We are proud of our team and continue to work hard to make sure we reflect the communities we serve.[26]

→ Investing in self-care makes our work more sustainable

Running an emergency response support line for human rights defenders and other at-risk groups from civil society can have a direct psychological impact on the well-being of the Helpline team. We have dedicated organizational resources to support the team's well-being and protect against burn-out, and are pleased to report that **more than 85% of all the cases managed by the Helpline to date were handled by team members who are still part of the team today.**

[25] Digital Security Helpline Community Documentation. https://communitydocs.accessnow.org.
[26] Access Now. Meet the Access Now Digital Security Helpline team: https://www.accessnow.org/about-us/?staff_team=helpline#staff.

CONCLUSION

One thing is clear: the global network of activists, journalists, human rights defenders, and civil society organizations is in ever-increasing need of digital security assistance as they face more severe and more persistent threats. Keeping civil society safe, connected, and empowered to do their work is an essential foundation for the broader fight to protect human rights in the digital age, and we all must rise to the challenge.

Calls for rapid digitalization should not come ahead of critical human rights protections — especially when implementation of more sophisticated technologies leads directly to a rise in digital authoritarianism. States must protect —not attack — their own populations. Companies must commit to respecting our human rights online. And civil society must recognize and respond to the inherent risks of online activities. Together, we can build a safer, more secure, free and open digital future for everyone.

We look forward to working closely with our growing network of partners and allies to further our mission of protecting human rights online and to develop new strategies for ensuring the digital security of people most at risk.

THANK YOU

We thank you for your trust in our work. We are grateful to our tireless and dedicated Helpline staff, to the rest of the Access Now team for their endless support, and to our partners who share our mission and collaborate with us. We look forward to continuing our collective efforts to ensure civil society and the users most at risk are able to freely and safely exercise their human rights, online and off.

CONTACT

For more information, visit https://www.accessnow.org/help
For digital security assistance, contact help@accessnow.org
For media inquiries, contact press@accessnow.org

accessnow

Access Now (accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.