yubico

CASE STUDY

ARTICLE 19 defends global human rights activism with YubiKeys

International human rights organization secures free speech advocates against state-sponsored cyber attacks

> Man-in-the-middle attacks are a good example why providing YubiKeys for the high-risk community is really helpful. An attack will be blocked immediately."
>
> **Mo Hoseini** | Head of Resilience | ARTICLE 19

Defending freedom of expression around the world

The Universal Declaration of Human Rights, agreed upon by the UN General Assembly in the aftermath of the second world war, enshrines the fundamental rights that all societies are required to uphold. Article 19 of the document covers the right to freedom of opinion and expression—and in 1987 this inspired the creation of a human rights organization devoted to defending that right.

For four decades, ARTICLE 19 and their network of partners have fought for a world where freedom of speech, and its champions, are not subject to repression. From Russia (where ARTICLE 19 has been declared an "undesirable organization") to Iran and beyond, ARTICLE 19 supports communities whose freedom of speech is under threat from authoritarian regimes.

"The work is important because we defend the rights of vulnerable communities across the globe," says Mo Hoseini, Head of Resilience at ARTICLE 19. "We work with governments to bring positive change. When change comes, societies struggle to digest that much freedom—so it's important to help introduce global standards and best practices from other regions."

Digital spaces increasingly targeted by cyber armies

ARTICLE 19 believes access to the internet is an important way to promote freedom of speech. Equally important, though, is that high-risk communities have the tools to be safe and secure online. "We've seen intelligence reports that regimes like Russia, China and Iran use cyber attacks, including phishing campaigns, to attack human rights activists," says Hoseini.

> For security agencies, the most convenient and affordable way to target activists is a cyber attack—usually a phishing attack."
>
> 
>
> **Mo Hoseini** | Head of Resilience | ARTICLE 19

Industry

- Non-profit

Protocols

- Passkeys
- 2FA

At a glance

- Founded in 1987
- Based in London
- Global presence through 9 international hubs

Key results

- Phishing-resistant authentication for Google Advanced Protection Program
- Drop in account takeovers reported by partner network
- Protection for ARTICLE 19's internal Microsoft ecosystem

Yubico solutions deployed

- YubiKey 5
- Security Key

Threats to civil society and human rights defenders are evolving. “20 years ago there were lots of direct physical threats. Now they are targeted by security agencies and their cyber armies,” says Hoseini. “Activists may be living abroad, but their entire soul is back home. Intelligence agencies are dying to know who they are talking to, so they can go after leaders on the ground.” In authoritarian regimes, the identities of local activists being exposed could result in arrest, detainment and even execution. In other cases, the goal can be to take over an activist’s public accounts in order to discredit them and others within their network.

The ‘Authoritarian Playbook’ targets human frailty

While awareness of cyber threats has improved, high-profile activists may have a false sense of security, and may not even realise when they’ve been targeted. “Attacks have become more sophisticated, and different regimes often use identical methods—this is all part of the ‘Authoritarian Playbook’.” says Hoseini.

The ‘Authoritarian Playbook’
How repressive regimes target activists with ‘man-in-the-middle’ attacks
Mo Hoseini, Head of Resilience, ARTICLE 19

1. **Social Engineering**
   “Attackers study you, they really go digging. They know what you're working on; they know your partner's name; they have a lot of information to design an attack. A colleague was targeted through threats and links sent to his wife’s work email.”

2. **Taking time to build trust**
   “Attacks have become harder to spot, and much more professional. They aim to build trust, sometimes over several days. The intention is to extract critical information from conversation, then move on to actually taking over an account.”

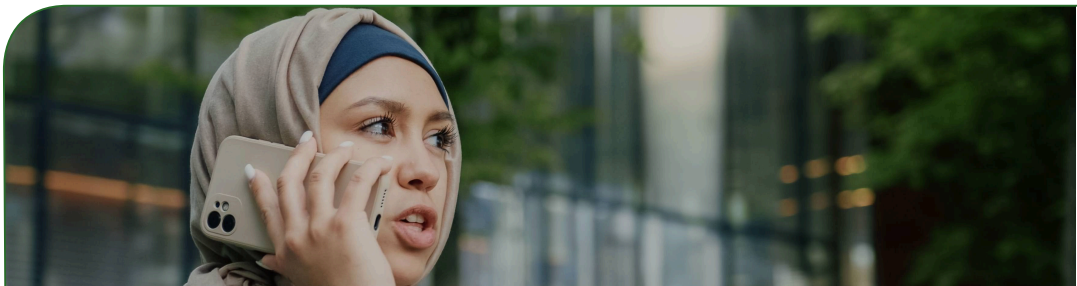
3. **Targeting tiredness**
   “A very common tactic is to contact you either very early in the morning or late at night. They will send a link to a fake landing page, with the goal of extracting your login credentials and MFA codes. When you can’t think straight, it’s harder to spot.”

The same kind of attacks have been identified across different countries, including during electoral campaigns. Activists and human rights defenders often use one email address for everything, whether online shopping or communicating with activist groups. This means that a breach of a single personal account can lead to the compromise of extensive activist networks.

Closing cybersecurity gaps with security keys

The solution is to protect accounts with multi-factor authentication (MFA), yet many common methods have still proven vulnerable. “In authoritarian countries, MFA using SMS is meaningless—governments and security bodies can demand that phone operators provide ‘back door’ access,” says Hoseini. Mobile apps offer an imperfect alternative. “High-risk communities often have outdated smartphones, potentially infected with Spyware.”

> “Studies show mobile authentication is breakable and not as safe. It's not as bulletproof as security keys.”
>
> **Mo Hoseini** | Head of Resilience | ARTICLE 19



Many human rights defenders supported by ARTICLE 19 protect themselves online with Google's Advanced Protection Program, which requires passkeys—either stored on a phone, laptop or security key—to authenticate. Google was the first to make ARTICLE 19 aware of the YubiKey, a phishing-resistant hardware security key that requires a physical touch, or contactless tap, to authenticate, effectively blocking any man-in-the-middle attacks. The YubiKey, manufactured in Sweden and the US, can store up to 100 passkeys, as well as Smart Card credentials and more.

At the time, ARTICLE 19 was designing a major project supporting a wide range of high-risk communities in the diaspora—and it was decided that this should include supplying YubiKeys to high-risk individuals. This was made possible due to Yubico's Secure it Forward program, which donates YubiKeys to non-profit organizations, human rights defenders and journalists around the world. "Part of choosing YubiKeys is down to the partnership," says Hoseini. "We see how Yubico has served the high-risk community."

> "It builds trust that YubiKeys are manufactured in Sweden and the USA. When talking about security, something that has critical access to your accounts, I would always go for something European-made."
>
> **Mo Hoseini** | Head of Resilience | ARTICLE 19

Securing global human rights defenders—one YubiKey at a time

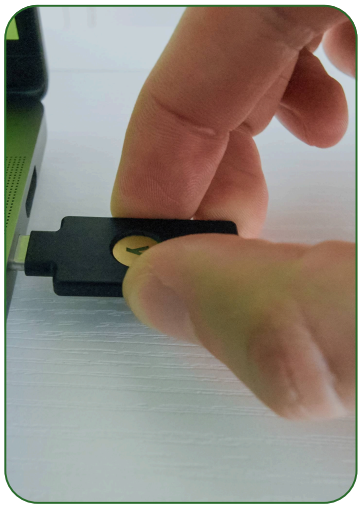
Since being introduced to the Secure it Forward program, ARTICLE 19 has distributed more than 1,000 YubiKeys to dozens of partner organizations and hundreds of human rights defenders. Many of these high profile activists live abroad and may be under government protection. "Security services still think in an old fashioned way," says Hoseini. "They protect their physical security, but often nothing is done to counter the digital threat."

To fill this gap, ARTICLE 19 provides training sessions to high-risk communities, an important part of which is introducing the importance of strong authentication and distributing YubiKeys to those in need. They also operate a 'Train the Trainer' program, so members of the activist community can distribute—as well as implement and set up—YubiKeys within their networks.

> "YubiKeys are easier than traditional MFA methods. It's very straightforward to set up"
>
> **Mo Hoseini** | Head of Resilience | ARTICLE 19

The results of ARTICLE 19's campaigns have been dramatic. "Prior to rolling out security keys across the community, we were getting many reports regarding government-sponsored attacks and requests for support when accounts were hacked," says Hoseini. "This has stopped, because 90% of civil society uses Google, and there's no way accounts can be taken over when using a YubiKey and the Advanced Protection Program—their accounts become bulletproof."

Users' experience of authentication has also improved. "Our partners are very comfortable with YubiKeys," says Hoseini. "It's easier for them than using traditional MFA methods." In addition to securing the Advanced Protection Program, YubiKeys are often used to protect password managers, or for passwordless access to the growing number of services supporting passkeys.



Building a safer future for global voices

ARTICLE 19 has also begun deploying YubiKeys to their internal team around the world, prioritizing regional offices at high risk. Their admin team, based in London, plans to change the preferred authentication method for the organization's Microsoft ecosystem, moving from Microsoft Authenticator to the YubiKey. Staff are also encouraged to use YubiKeys to protect their personal email and any social media accounts.

Staff are given the YubiKey 5 Series, with USB-C and NFC capability allowing the option of authenticating both by inserting the YubiKey or tapping it against a device's NFC reader. Two YubiKeys are provided—one to keep with them at all times, and a second as backup to store at home to prevent lock-outs in case the first is lost or damaged.

Once YubiKeys are deployed to every employee, ARTICLE 19 hopes to continue securing more partners around the world—and not just those at highest risk. As phishing attacks become more sophisticated, security services seek out the weakest link in an organization's extended network. This makes the mission of securing all accounts with phishing-resistant authentication more important than ever.

> "There's no way accounts can be taken over when using a YubiKey and the Advanced Protection Program—their accounts become bulletproof."
>
> **Mo Hoseini** | Head of Resilience | ARTICLE 19

Learn more | yubi.co/customers | yubi.co/contact

yubico

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA). The company is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com.