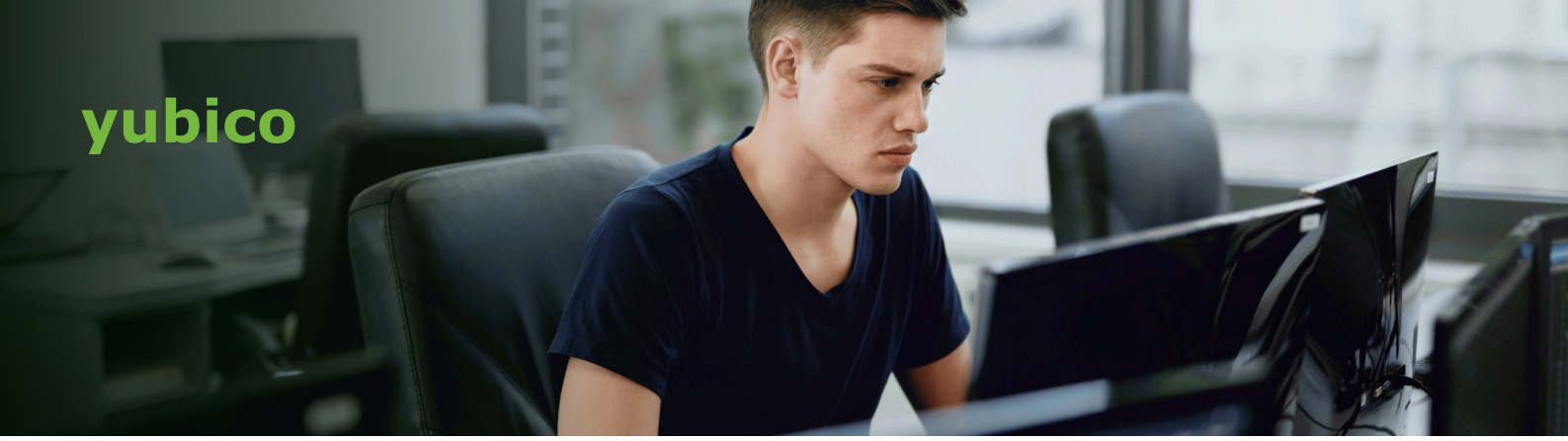


yubico

CASE STUDY

RESIDENT.NGO

Industry

- Non-profit

Protocols

- FIDO U2F

At a glance

- Digital security assistance for non-profits and independent media
- Capacity-building to protect high-risk groups against state-sponsored attackers
- Based in Vilnius, Lithuania

Key results

- 1,500+ YubiKeys distributed to high-risk groups in Eastern Europe
- Enabled phishing-resistant MFA for Google Advanced Protection Program (APP)
- Zero account takeovers among organizations protected by YubiKeys

Yubico solutions deployed

- YubiKey 5C NFC
- YubiKey 5 NFC
- Secure it Forward program

RESIDENT.NGO stops state-sponsored phishing attacks and defends democracy with YubiKeys

Empowering journalists and activists to combat cyber espionage amid rising authoritarianism

> "If you are a high-risk organization, and you believe state-sponsored hackers are going to attack you, phishing-resistant MFA is needed. The easiest way to implement that is YubiKeys."

Mykola Kostynyan | Co-founder | RESIDENT.NGO

Strengthening digital resilience for independent media and NGOs in Eastern Europe

RESIDENT.NGO is a non-profit group of security practitioners dedicated to strengthening the digital resilience of pro-democracy organizations across Eastern Europe. They focus on building organizational capacity and providing practical solutions tailored to the specific needs of non-governmental and media organizations, human rights defenders, journalists and activists.

Co-founder Mykola Kostynyan is part of the RESIDENT.NGO threat lab, which is focused on researching, identifying and responding to evolving digital threats. "We are digital security practitioners working with civil society and independent media organizations in Eastern Europe for more than ten years," says Kostynyan. "We established RESIDENT.NGO to provide continuous and sustainable support where we see that it is needed."

Digital attacks from state-sponsored hackers threaten democracy

Eastern Europe is a stage for geopolitical conflict, with an increasing number of repressive states seeking to consolidate power and repress dissenting voices. In authoritarian states, pro-democratic groups—including investigative journalists, election monitors, anti-corruption and eco-activists and LGBTQ+ organizations—are seen as a direct threat to government power. They are closely monitored, and at constant threat of smear campaigns, arrest and imprisonment. Law enforcement agencies frequently raid offices and confiscate IT equipment, while those in hiding or in exile abroad face remote cyber attacks.

Cyber attacks also play an increasing role in inter-state conflict. Russia is known to use state-sponsored hacker groups in its attempts to influence and control the politics of other countries in the region, particularly during election cycles. In September 2025, Moldova's electoral commission was revealed to have suffered cyber attacks days ahead of voting.[1] "Russian state hackers are usually part of the security apparatus," says Kostynyan. "It's another dimension of war—a war in cyber space."

[1] https://www.politico.eu/article/moldova-electoral-commission-cyberattack-days-ahead-vote-russia-democracy-doina-nistor/

> The top three remote attacks are phishing, phishing and phishing."
>
> **Mykola Kostynyan** | Co-founder | RESIDENT.NGO

As freedoms decline—pro-democratic forces must unite in response

The impact of successful cyber attacks can be immediate, and direct. Kostynyan gives an example: "if the email of an organization supporting human rights defenders in Belarus is hacked, there could be 15 local activists thrown in jail the next day." In the long term, the power to restrict pro-democratic forces, even outside the country, can strengthen authoritarianism.

Over the years, Kostynan has seen democracy decline across Eastern Europe—and worse, authoritarian countries have worked together on strategies to repress dissent. "As activists left Belarus, the government began to use cyber attacks against those abroad. Now, those same things which took ten years to implement in Belarus are implemented in six months in Georgia."

> States are no longer pretending to be democratic. They aren't afraid to do things they couldn't in the past."
>
> **Mykola Kostynyan** | Co-founder | RESIDENT.NGO

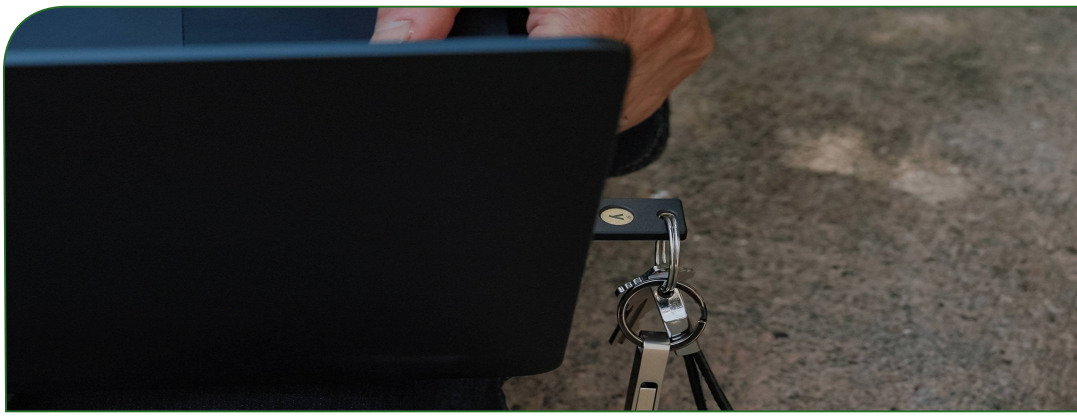
As authoritarian states ramp up their capabilities, it is essential for those under threat to work together. "The problem is that independent organizations are small and have limited resources, while they are up against the attackers who are hacker groups sponsored by the state," says Kostynyan. "It's important we build up our own capacity. We are actively sharing experiences and best practices to support civil society against the threat actors."

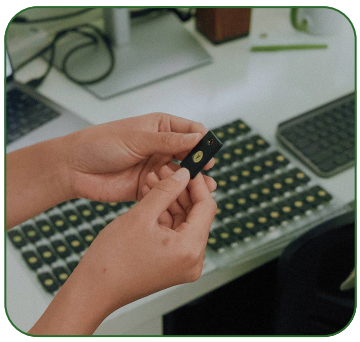
Secure authentication plays a vital role in cyber defense

While awareness of cyber threats, and forensic analysis capacities, have grown in recent years, especially in Ukraine, RESIDENT.NGO saw that authentication posed a security gap for many of the high-risk organizations they work with. Legacy MFA methods, including SMS and authenticator apps, are not phishing-resistant, and can be easily intercepted or bypassed. Many frontline civic groups lack the capacity and funds to implement and maintain device management solutions—ruling out mobile authenticators.

Cyber attacks are also growing in sophistication. "Phishing attacks that bypass second factors on mobile authentication used to be super rare—now it's the new normal," says Kostynyan. A prominent example is the "River of Phish" incident, a sophisticated spear-phishing campaign launched by Russian hackers in Eastern Europe in 2024.

RESIDENT.NGO participated in an investigation into the incident. The vulnerabilities discovered led co-investigators Access Now and Citizen Lab to note that multi-factor authentication is "one of the most powerful ways to protect your account from getting hacked", recommending passkeys, in particular those stored on hardware security keys. "A user was tricked into giving away a code from their authenticator app; it wasn't phishing-resistant" says Kostynan. "Hardware security keys are phishing-resistant, because you can eliminate the human factor."





“YubiKeys eliminate the human factor. Even if a user believes that a phishing site is a real website, their YubiKey will simply not work there. This is something we really like.”

Mykola Kostynyan | Co-founder | RESIDENT.NGO

YubiKey, a modern security key, stops phishing in its tracks

The YubiKey—a hardware security key that requires a physical touch or contactless tap to authenticate—effectively blocks the methods used in the ‘Rivers of Phish’ attack. Manufactured in Sweden and the US, a single YubiKey can store up to 100 passkeys, Smart Card credentials and more, allowing users to secure all their essential digital services.

“The victims of the ‘Rivers of Phish’ hack were a kind of role model: regular training, cyber awareness and widespread MFA adoption. We realised that without security keys it is no longer enough, absolutely not enough.”

Mykola Kostynyan | Co-founder | RESIDENT.NGO

THE ‘RIVERS OF PHISH’ CAMPAIGN[2]

The ‘River of Phish’ campaign was a 2024 spear-phishing campaign attributed to the Russian threat group COLDRIVER (also known as STAR BLIZZARD or SEABORGIUM).

Attacks targeted international NGOs and civil society organizations across Eastern Europe, as well as Russian and Belarusian independent media and activists living in exile.

Social engineering and fake login pages harvested credentials, with the primary objective being cyber espionage—stealing sensitive data about staff, activities, sources and confidential communications to disrupt operations, discredit organizations or endanger personnel.

Secure It Forward Program delivers 1,500+ YubiKeys to high-risk activists

RESIDENT.NGO opted to deploy the YubiKey across their network of high-risk organizations. Kostynan had long known about their ability to offer easy-to-use phishing-resistant protection. It wasn’t until Global Gathering, an international event focused on technology and human rights, that he was made aware of Yubico’s Secure it Forward program, which donates YubiKeys to high-risk groups including non-profit organizations, human rights defenders and journalists worldwide, helping those most at risk improve their security posture.

YubiKeys are particularly important as RESIDENT.NGO recommends that high-risk organizations implement the Advanced Protection Programme (APP), Google's highest level of account security intended for users at elevated risk. The APP mandates passkeys—like those stored on the YubiKey—for authentication, blocking less secure two-step verification methods like SMS or standard TOTP codes. The APP also strictly controls third-party app access to sensitive data and employs enhanced, more difficult account recovery protocols to thwart attackers.

[2] https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/

Those protected with YubiKeys and the Google Advanced Protection Programme have not been hacked. It's a good result."

Mykola Kostynyan | Co-founder | RESIDENT.NGO

Since 2024, RESIDENT.NGO has received more than 1,500 keys through the Secure It Forward program. They distribute YubiKeys to organizations in Lithuania, Poland, Georgia, Ukraine and Moldova, as well as Belarusian activists in exile. RESIDENT.NGO targets organizations with a security point person who will be able to implement and be responsible for the YubiKeys.

As part of their training and ongoing support, RESIDENT.NGO encourages recipients to use YubiKeys as a second factor for work accounts on Google and for private accounts on services like Facebook, Yahoo, Dropbox, Proton Mail, and Apple accounts. Training emphasizes that the YubiKey should be kept on the user's person at all times, especially since journalists and human rights defenders are often on-the-move, working remotely. Kostynan also hopes that the communication app Signal, which is popular across the region due to its end-to-end encryption, will soon integrate authentication with truly phishing-resistant methods, including the YubiKey.

Zero account takeovers with YubiKeys sets a solid foundation for a phishing-resistant future

Deployment has proved a success—evidenced by the fact that protected organizations frequently ask for more YubiKeys for their new staff members. Most importantly, there have been no account takeovers against users protected by YubiKeys and Advanced Protection Program.

The Google for Nonprofits program, which offers Google Workspace without charge to eligible organizations, recently became available across Eastern Europe, including in Moldova, Armenia and Georgia. "This is a new beginning for both organizational infrastructure and ways to secure it," says Kostynyan. "YubiKeys with the APP mean Google Workspace is something we can really make phishing-resistant. It's a new start for the region."

Looking forward, the goal for RESIDENT.NGO is the widespread adoption of phishing-resistant MFA among vulnerable organizations across Eastern Europe. Kostynyan's advice for such organizations, especially those at risk of state-sponsored attacks, is to deploy phishing-resistant MFA, and that the easiest way to implement it would be the YubiKeys. Only by following best-practices like the adoption of highest assurance security can activists in Eastern Europe defend against the threats of authoritarian regimes—and continue the fight for democracy.

> Our experience with the Secure it Forward program was easy and friendly—it couldn't have been better. We needed the YubiKeys, we requested them and we received them. Simple and efficient."

Mykola Kostynyan | Co-founder | RESIDENT.NGO

[2] https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/

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.