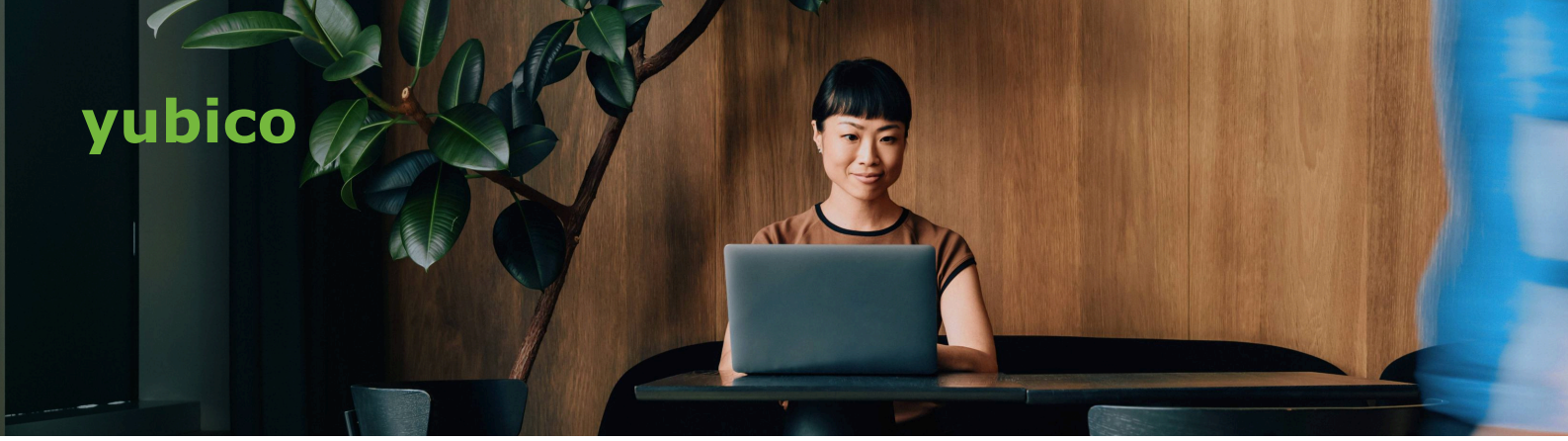


CASE STUDY

OCCRP

Industry

- Non-profit media

Protocols

- FIDO
- OpenPGP

At a glance

- Investigative journalism staff on six continents
- 70+ media member centers enabling truly global reportage
- Open source data platform with more than 4.5 billion records

Key results

- Strong authentication for Google's Advanced Protection program
- Secures Single Sign-On to web services
- Highest assurance protection against sophisticated phishing attacks

Yubico solutions deployed

- YubiKey 5 Series

Preventing Attacks on Journalism: YubiKeys Secure OCCRP's Mission to Expose Crime and Corruption

> When security is hard, people find ways around it. When it's easy, they'll use it. That's one of the nice things about YubiKey: just plug it in and touch it. It's easy and it's effective."
>
> **Geoff Hunter** | CTO & CISO | OCCRP

Fighting for Truth in a Hostile Environment

The Organized Crime and Corruption Reporting Project (OCCRP) is one of the world's largest investigative journalism organizations, whose stories—published independently and in partnership with media outlets—hold the powerful to account. Since its founding in 2007, OCCRP's work has helped return more than $11 billion to the public sphere, and resulted in more than 700 indictments, arrests and sentences. Recent stories have uncovered an empire of scam call centers across Europe and Israel, how Balkan criminals planned brutal murders by phone and how dirty money is invested in Dubai real estate markets.

In addition to OCCRP's mission-driven non-profit newsroom, it provides global members with tools, resources and support for investigations. The organization's open-source Aleph platform allows journalists and publications around the world to access an archive of more than 4.5 billion documents acquired from databases, leaks and investigations.

Geoff Hunter serves as Chief Technology Officer and Chief Information Security Officer. He is responsible for ensuring OCCRP's global team of journalists and staff are enabled with the right tools to succeed—including making sure that they, and their data, remain secure. "Technology and security go hand in hand," says Hunter. "Security is fundamental to everything we do."

Due to the type of reporting OCCRP does and the countries in which they work, there is a very real threat to the lives of journalists—a fact that forms the basis of Hunter's entire strategy. "We worked with a journalist who was killed because of his investigative reporting," says Hunter. "Security is vital because of this substantial risk to life. It's an incredible stress that forces us to strategize on a daily basis."

> Security here isn't just about protecting yourself; it's about protecting your colleagues, your sources, your friends, and your family. That makes it an easy conversation."

Geoff Hunter | CTO & CISO | OCCRP

Digital attacks provide criminals with the sensitive information they need to carry out a physical attack against journalists or their sources. According to Hunter, the most common attack vector is sophisticated spear phishing directed at specific targets. “Well crafted spear phishing builds trust between individuals before there’s any call to action to do anything that’s going to compromise you,” says Hunter.

To counter these threats, many of which originate from nation states, Hunter’s team puts a strong emphasis on multi-factor authentication (MFA) for online accounts. Having fallen victim to advanced Spyware like Pegasus in the past, Hunter is concerned that phones may be compromised in some cases. This means that any mobile-based MFA, such as Time-based One-Time Passwords (TOTP) and authentication apps, could also be compromised.

> “It’s an incredibly hostile environment and we are frequently targeted. The people we’re investigating are either organized crime or hostile nation states. And even nation states who technically should be friendly on paper can be hostile to what we do.”
>
> **Geoff Hunter** | CTO & CISO | OCCRP

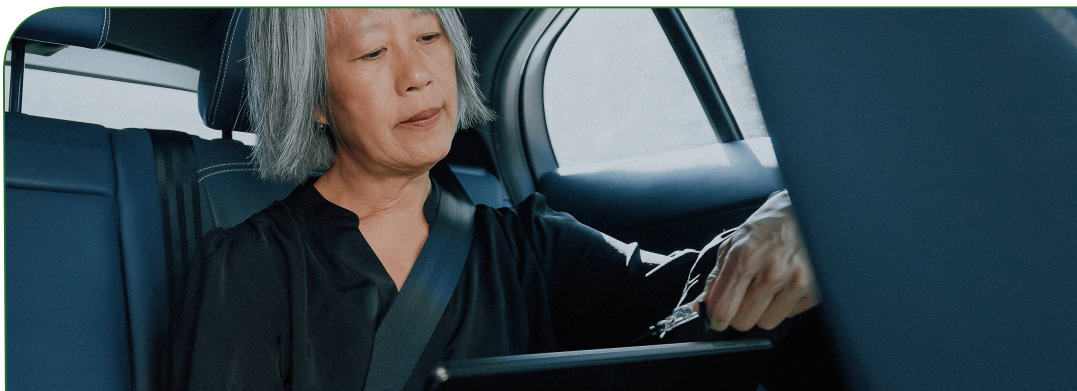
The YubiKey Simplifies Phishing-Resistant Authentication

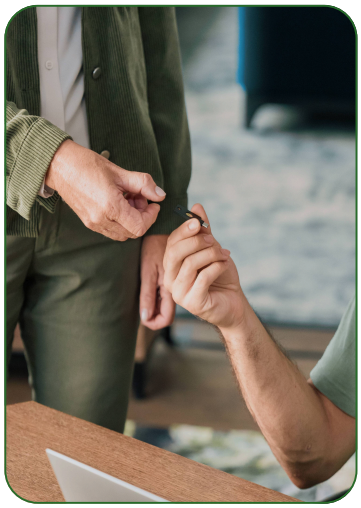
Historically, TOTP codes had been widespread across OCCRP for all employees. Aware of the risks of legacy phone-based authentication, OCCRP opted to deploy the YubiKey, a hardware security key that counters phishing attacks by requiring physical touch. When Hunter arrived at OCCRP, he was pleased that YubiKeys were already in place. “Being in the security space, I remember buying a couple of YubiKeys when they first came out,” says Hunter. “It's just ubiquitous now as far as we're concerned—it’s the obvious thing to have.”

The initial use case for YubiKeys at the organization was to work in conjunction with Google’s Advanced Protection program, which requires high-risk users to use FIDO authentication, with a passkey or security key, for account security. YubiKeys are also used at OCCRP for privileged access and as a second authentication factor for various web services through OCCRP’s Single Sign-On service.

The YubiKey allows users to leverage multiple protocols, to match the use case and tech-saviness. “If you’re someone like me,” says Hunter, “you can set up all sorts of clever stuff with them. Some of the IT team will store PGP keys on the YubiKeys, but that isn’t mandated. All the average user has to do is plug in and touch their YubiKey—it’s not hard.”

> “Anything that prevents account compromise is important, and TOTP is fine, but you can’t beat a hardware security key. You just can’t. Anyone who’s using the YubiKey over TOTP is better protected.”
>
> **Geoff Hunter** | CTO & CISO | OCCRP





Secure It Forward Donations Enhance Security for High-Risk Users

OCCRP was able to benefit from Yubico's Secure it Forward program, which donates YubiKeys to non-profit organizations, human rights defenders and journalists around the world, helping those most at risk improve their security posture. While YubiKeys have not been deployed fully across the organization, with many lower risk users still relying on mobile authentication, Hunter hopes for a day when they are deployed both for everyone at OCCRP and the entire member network.

User feedback has been positive. "We encourage people to use YubiKeys and when we've given them out people love them," says Hunter. "It's another tool, just like a pen or a notebook. We encourage users to use YubiKeys for their personal accounts as well. We push the message of strong authentication as part of our security awareness training very hard because it is so vital. We do a lot of outreach."

Looking Ahead to Going Passwordless

An end goal for Hunter is for OCCRP to adopt fully passwordless authentication, boosting both ease-of-use and phishing-resistance. The YubiKey offers a helpful alternative to biometric-based authentication, as journalists travelling in certain jurisdictions may face their biometric data being confiscated without warning. These concerns highlight the risks that OCCRP and its network face every day in their work. When fighting for truth, and exposing the crime and corruption of the powerful, the stakes couldn't be higher—and only the strongest security will do.

> We'd like everyone to have a YubiKey. Having a physical second factor is such a good tool against phishing and account compromise. It's pretty much unbeatable."
>
> **Geoff Hunter** | CTO & CISO | OCCRP

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.

© 2025 Yubico