

## CASE STUDY

---



### Industry

Non-Profit

### Benefits

DDC equips campaigns of all sizes with phishing-resistant MFA, ensuring they remain digitally secure.

### Protocols

2FA, PGP

### Products

YubiKeys 5 Series  
Yubico Security Keys

### Deployment info

Campaigns across all parties are trained to leverage YubiKeys, with tens of thousands already deployed.

---

## Defending Digital Campaigns secures electoral campaigns with YubiKeys

In the high-stakes world of political campaigns where every decision can tip the balance, cybersecurity isn't just a technical detail—it's a critical safeguard for the democratic process. As election interference becomes more sophisticated, organizations like Defending Digital Campaigns (DDC) are stepping up to ensure that campaign teams across the political spectrum are equipped with the tools they need to protect their most sensitive information. Through their strategic partnership with Yubico and its Secure It Forward program, DDC is doing more than just defending campaigns against those who wish to disrupt them. They're protecting the pillars of democracy itself.

“YubiKeys gets people to a much higher state of security right away. That's why it was important to work with a company like Yubico, why a product like the YubiKey is so important and why we wanted them in campaigns.”



**Michael Kaiser** | President and CEO | DDC

### Securing democracy means securing electoral campaigns

DDC is a nonprofit C4, nonpartisan and non-aligned organization providing electoral campaigns access to cybersecurity products, services and information regardless of party affiliation. Because campaigns are subject to strict finance laws and contribution reporting standards, the organization has been granted special permission by the Federal Election Commission to make their services available to federal campaigns free from reporting the value of the in kind donation. DDC also provides education and information about risk and implementing cybersecurity across a broad range of people in the stakeholders in the political sector. Additionally, DDC is currently approved to provide the same services down ballot in Georgia, Michigan, Ohio, and Virginia with more states providing approvals in the near future.



Their work is critically important for safeguarding democracy and election fairness, especially in an age where political campaigns face increasing threats from those looking to cause disruption, instability and chaos. Most electoral campaigns in the United States are small operations; they are nimble with an extraordinary amount of competing priorities. And, they're regular targets for bad actors, rogue nation states and groups of "Hacktivists" seeking what they believe to be social justice by influencing electoral outcomes. These criminals are well organized, and their impact has been significant in recent years, as notable instances of cyber interference within campaigns have been reported for every US presidential election since 2012<sup>1234</sup> and across elections nationwide at every level.

According to the DDC every campaign, every campaign worker and everybody who works in a political organization that's associated with campaigns is considered to be high-risk computer users.

“ They are higher risk than your average computer user, which is one of the reasons that we've often talked about the strongest form of authentication being security keys, because with high risk comes the need for the highest level of protection you can get.”

**Michael Kaiser** | President and CEO | DDC

As it's often sensitive personal or financial information these criminals seek, the account credentials of campaign staffers are prime targets. Email login details are top prizes, but not the only inroad for gaining access to campaigns. "We know that accounts themselves are vulnerable," says Kaiser. "They're the main target of the bad actors trying to get into someone's Cloud accounts. Social accounts are always going to be very, very high on the bad actors list for a whole host of reasons. We always knew that we wanted to implement and get campaigns to implement the strongest authentication possible."

### Securing high risk users a top priority

Campaigns need a way to secure themselves quickly and to the highest possible levels without losing their momentum. However, many prefer to spend their limited budgets on ads and other promotional activities instead of focusing on cybersecurity. DDC sees it as their mission to raise awareness for cybersecurity with campaigns teams and to support them in becoming more secure.

“ From the very beginning at DDC, it was understood that strong authentication and account protection was always going to be one of the number one things that we recommended to all campaigns.”

**Michael Kaiser** | President and CEO | DDC

<sup>1</sup> BBC, South Korea's spy agency admits trying to influence 2012 poll, (August 2017)

<sup>2</sup> FBI, Russian Interference in 2016 U.S. Elections

<sup>3</sup> DHS, Key Findings and Recommendations: Foreign Interference Related to the 2020 US Federal Elections, (March 2021)

<sup>4</sup> U.S. Department of the Treasury, Treasury Takes Action as Part of a U.S. Government Response to Russia's Foreign Malign Influence Operations, (September 2024)

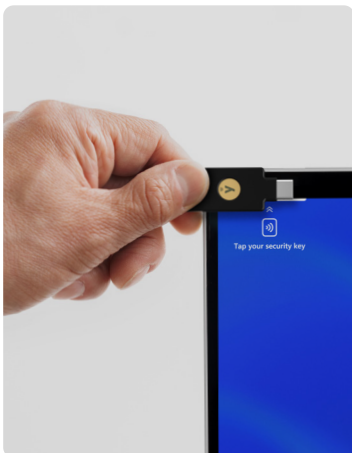
Working with Yubico, a leader in authentication, was therefore a natural choice.





Yubico was one of the earliest companies we worked with. Clearly, strong authentication was going to be one of the core things that we focused on. Many of the people that we were talking to in the political sector were already aware of the importance and need for security keys and using security keys.”

**Michael Kaiser** | President and CEO | DDC



Reiterating the need for security keys in this sector is Tiffany Schoenike, who runs strategic initiatives at DDC. According to her, while security cannot help win a campaign, it certainly can help lose a campaign.



Campaigns need support in different ways, and that’s why there are different risk profiles for different campaigns—from a presidential campaign on down ballot. They are going to have different cybersecurity needs. But for every single campaign, we recommend enabling a security key. That is the number one thing.”

**Tiffany Schoenike** | Strategic Initiatives | DDC

### YubiKeys provide ironclad security for electoral campaigns

Partnering with Yubico and its [Secure It Forward](#) program, which donates YubiKeys to mission-driven organizations most at risk, means that DDC is able to get the strongest authentication possible directly into the hands of campaign professionals. First, DDC sends their campaign partners a special code for the Yubico online store that allows them to order YubiKeys for their entire team, free of charge. This is all facilitated by the [Secure It Forward](#) program in a rapid and efficient manner.



One of the things that campaigns really appreciate is how quickly we can send them keys. If they order them at nine in the morning, they can have the key codes a few hours later and Yubico actually sends them the [physical] key overnight. It’s a wonderful thing, and one of the reasons why we say the YubiKey is the number one solution.”

**Tiffany Schoenike** | Strategic Initiatives | DDC

Once the keys are delivered, DDC has an onboarding team who gets the campaign’s staff up and running by demonstrating the various ways to implement their new YubiKeys across the platforms they use including their emails, computer logins, social media accounts, Microsoft or Google ecosystem and beyond. One of the biggest educational moments is helping these professionals understand that they don’t need a key for each account; it’s one key for multiple accounts.



YubiKeys allow us to say, ‘Take a key and protect your work email account, protect your Cloud account, protect your social account, and protect your personal email account,’ all of those are things that people can do quickly to really up their authentication to the strongest level possible..”

**Michael Kaiser** | President and CEO | DDC

The YubiKey’s simple user experience has user buy-in and adoption amongst campaign staff, thereby elevating their security posture. With Yubico’s support, DDC has contributed tens of thousands of YubiKeys to campaigns and their staff over the past five years



### DDC secures its own distributed workforce with YubiKeys

But it's not just DDC's campaign partners who benefit from having the strongest form of MFA possible. DDC purchases its own YubiKeys to secure its distributed, remote team. Cloud-based services play a major part in DDC's day-to-day operations, so providing its staff with a security key linked to the accounts they use on behalf of the organization is the perfect solution when using personal devices.

Nonprofits don't differ much from campaigns when it comes to compliance, as neither are beholden to specific regulations regarding cybersecurity. However, having the most secure form of MFA in place has not only positively impacted the organization's cyber insurance costs, but also enabled DDC to set a strong example for their campaign partners.

“ You do get some of that institutional push down to make sure that you're doing the right thing as a security nonprofit, and we have to think about our own security. We have to walk the walk.”

**Michael Kaiser** | President and CEO | DDC

### Securing democracy now and into the future

In an era where digital threats loom large, the commitment to cybersecurity is not just about protecting information—it's about preserving the very foundations of democracy. Through their partnership with Yubico and support from its Secure It Forward program, DDC not only equips campaigns with top-tier security tools but also embodies the very principles they advocate for.



We're confident that our information is secure because we use YubiKeys.

**Tiffany Schoenike** |  
Strategic Initiatives | DDC



[Learn more](#)

[yubi.co/customers](https://yubi.co/customers)

[yubi.co/contact](https://yubi.co/contact)

**yubico**

Yubico (Nasdaq First North Growth Market 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](https://www.yubico.com).

© 2024 Yubico