yubico

Modernizing election security with the YubiKey

Highest-assurance multi-factor authentication

The election ecosystem is a prime target for cyber security threats and multi-factor authentication (MFA) is an IT security best practice that states and counties should deploy.

Leading up to the 2020 U.S. presidential election, Secretaries of State, election commissioners, election directors and information officers need to ensure the strongest possible IT security to ensure voter registration databases, voting infrastructure, election night reporting, and other critical systems are protected.

Not all MFA is equal

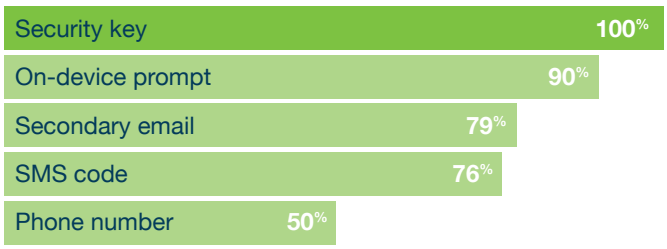
Usernames and passwords are insecure forms of authentication. The EI-ISAC recommends using MFA for account access, in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-63B and best practice #24 from the CIS Handbook for Elections Infrastructure Security.

Different types of MFA are available today such as SMS codes, one-time passcodes, or on-device prompts via mobile authenticators. But these methods are susceptible to breaches, phishing, and man-in-the-middle attacks. Mobile authenticators also make states and counties liable for mobile related costs, and importantly, considerably degrade the user experience.

YubiKeys are proven to stop account takeovers

Using hardware security keys like the YubiKey for MFA has proven to be the only solution to completely stop account takeovers, according to research by Google, NYU, and UCSD.

Account takeover prevention rates



Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

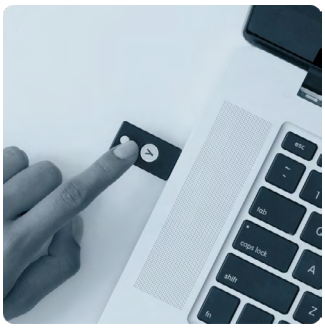
U.S. State uses YubiKeys to protect voter registration database

Concerns over database hacking motivated state elections office to look at more secure methods of authentication. They needed a solution that met the state's top three requirements: compliance with industry security standards, cost control, and ease-of-use. Other MFA options either didn't meet compliance requirements or were too cumbersome for the end user. The YubiKey met all of the state's top requirements for meeting compliance standards, budget constraints, and simplicity. 1,000 YubiKeys were deployed to employees accessing the voter registration database in all counties across the state.

YubiKeys offer a better user experience than mobile authenticators

YubiKeys are great for areas where mobile devices are prohibited, hard to use, or where connectivity is an issue. They have no breakable screens or batteries, and don't require connectivity to work. Authenticating with a YubiKey is as simple as inserting/tapping the key and touching it.

Secure access with YubiKey



Computers
Insert your YubiKey and touch it!

Mobile
Just tap it!

Benefits of the YubiKey for the election process:

- YubiKeys offer government compliant MFA. YubiKey 5 FIPS Series keys are appropriate for government officials, and Security Key Series keys are appropriate for election workers. The YubiKey 5 FIPS Series keys are FIPS 140-2 validated to meet the highest authentication assurance level 3 requirements (AAL3) of NIST SP800-63B guidelines, and are WebAuthn, FIDO and DFARS/NIST SP 800-171 compliant.
- Unlike mobile authenticators, YubiKeys offer a frictionless MFA user experience—users login with a single touch or tap which is 4 times faster than receiving and typing a code delivered by SMS.[1]
- YubiKeys drive high security ROI on MFA projects. Organizations have seen a 50% reduction in time to authentication compared to mobile authenticators and a 92% reduction in help desk costs.[2]
- YubiKeys support a number of open industry security standards including FIDO U2F and FIDO2, which makes them easy to integrate into existing environments.
- YubiKeys can be easily numbered, tracked, and managed as a state asset. If an employee leaves, the YubiKey can be quickly and securely reassigned to another user.
- YubiKeys can be distributed directly to election workers via Yubico logistics experts.
- YubiKeys are produced in the USA, maintaining security and quality control over the entire manufacturing process.

Protect voter registration databases and e-pollbooks

Voter registration databases are a high-value target for attackers looking to disrupt democratic processes. If logins aren't sufficiently secured, hackers can steal, corrupt or manipulate the integrity of sensitive voter data. The YubiKey provides strong hardware-based authentication to secure voter registration databases against hacking, and complies with the EAC recommendation that only authorized personnel should have access to the voter registration database.

Secure election management and reporting systems

The EAC checklist for securing election night reporting (ENR) systems suggests using two-factor authentication for uploading the results and for remote administration of ENR. The YubiKey offers highest-assurance two-factor authentication for access to the ENR application, election management systems, and to devices through which these systems are accessed such as laptops, desktops, and mobile devices.

Ensure election email confidentiality

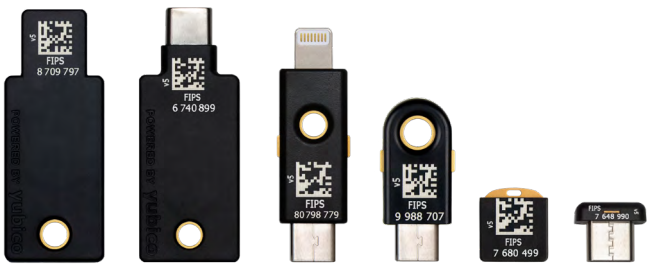
Foreign hackers are known to use email to infiltrate the political ecosystem. The YubiKey offers an added level of security for sensitive and confidential email communications. It is proven to eliminate phishing and account takeovers across GSuite, Microsoft Outlook, and Microsoft Office 365.

Protect election networks with the trusted leader

Yubico enables state government agencies to meet the highest authenticator requirements. With the ease of YubiKey deployment, election officials can stand up MFA protection well in advance of the 2020 general elections. Yubico is a leader in authentication security and the company's technology is deployed by state governments and federal agencies in the United States and around the world.

Learn more about how YubiKeys secure sensitive government information across election networks and political campaigns here.

1. Google defends against account takeovers and reduces IT costs
2. Ibid.



About Yubico Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with headquarters in Sweden and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at www.yubico.com.

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088