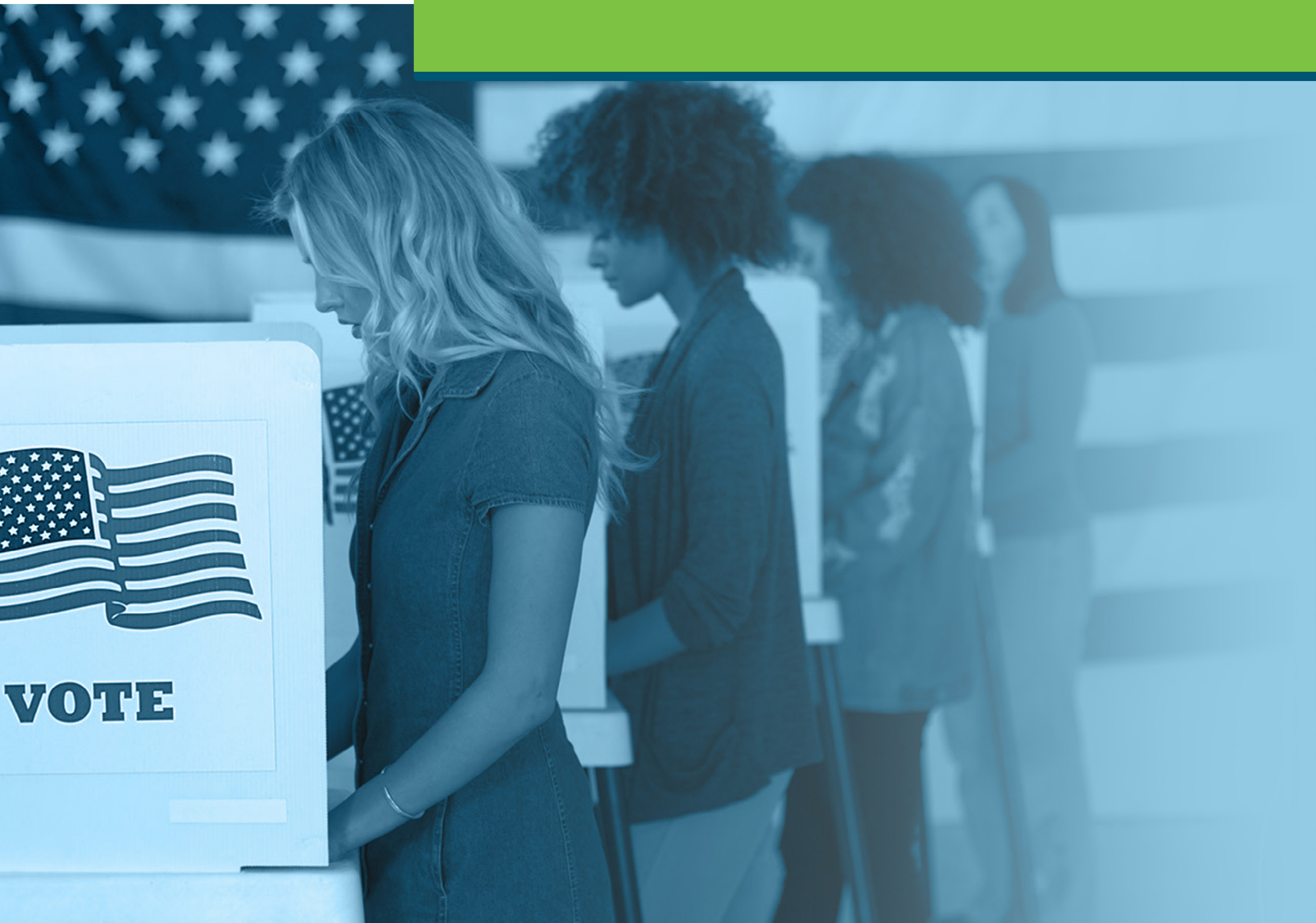
yubico

2024 SURVEY

Yubico, Defending Digital Campaigns and OnePoll

Impact of cybersecurity and AI on the 2024 election season



Executive Summary

The Yubico and Defending Digital Campaigns (DDC) survey, ‘Impact of cybersecurity and AI on the 2024 election season’ conducted by OnePoll polled 2,000 registered voters in the U.S. to better understand how voters perceive cybersecurity ahead of the 2024 U.S. elections, the impact of Artificial Intelligence (AI) and the concerns they have about the cybersecurity of political campaigns, regardless of party affiliations.

Although political parties may not be aligned on all matters, the new research finds that they do agree on one thing when it comes to cybersecurity: **AI will have a negative effect on the outcome of this year’s election.**

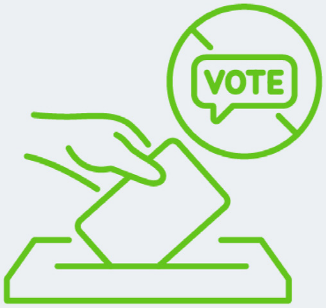
2,000

registered voters in the U.S.

The purpose of this study was to understand how registered voters perceive the cybersecurity of political campaigns and elections, and how those beliefs shape their voting habits and trust in political candidates. Our research indicates 42% of those who have donated to a campaign said their likelihood of donating again would change if the campaign was hacked and 30% report this would even change the likelihood of a candidate receiving their vote.

42%

of those who have donated to a campaign said **their likelihood of donating again would change if the campaign was hacked**



And **30%**

report this **would even change the likelihood of a candidate receiving their vote**

52%

of respondents **have received an email and/or text message** appearing to be from a campaign that **they suspected was actually a phishing attempt**

Because campaigns are built on trust, potential hacks like fraudulent emails, AI-generated content spreading misinformation and messages sent out impersonating political candidates via their social media accounts where they are directly interacting with their audience, could be detrimental to campaigns. The study showed bi-partisan agreement: Democrats (79%) and Republicans (80%) are both concerned about AI-generated content being used to impersonate a political candidate or create inauthentic content. They also believe that AI will have a negative effect on this year's election outcomes (42% and 49%).

Political campaigns often have access to personal information of voters and donors, which can be a treasure trove of data for a potential hacker. With all of this personal identifiable information (PII), one would think that political campaigns are taking all the right steps to not only protect this data, but also reassure voters that they have safeguards in place. Yet this study found that 85% of respondents don't have a high level of confidence that political campaigns effectively protect the personal information they collect.

85%

of respondents **don't have a high level of confidence that political campaigns effectively protect the personal information** they collect

Over

78%

of respondents are concerned about **AI-generated content being used to impersonate a political candidate or create inauthentic content**

And

43%

of respondents believe that **AI-generated content will negatively affect the outcome of the 2024 election**

Other key findings related to trust amongst voters include:

- 42% of those who have donated to a campaign said their likelihood of donating again would change if the campaign was hacked, and 30% report this would even change the likelihood of a candidate receiving their vote.
- When an audio clip with an AI voice was played, 41% believed the AI voice was authentically human.
- Over a quarter of respondents (26%) claimed that when donating to a campaign online, they have not completed the transaction because they were concerned about the security of the transaction or how their personal information would be handled.

To remedy this, registered voters would like to see campaigns and candidates taking precautions to prevent their websites from being hacked (42%) and using strong security measures like multi-factor authentication (MFA) on their accounts (41%).

42%

Preventing websites from being hacked

and

41%

using strong security measures like multi-factor authentication on their accounts

For more information on Yubico, visit yubico.com. To learn more about Defending Digital Campaigns programs, visit https://defendcampaigns.org.

With election season underway, what can campaigns do to protect themselves and build trust with voters? Even though cybersecurity attacks are becoming more sophisticated with tools like AI, there are simple ways to help mitigate these risks, including using strong, unique passwords and storing them in a password manager, along with enabling multi-factor authentication whenever possible using physical security keys like those available from Yubico and the DDC.

DDC, a nonprofit and nonpartisan organization, is committed to bringing cybersecurity tools and resources to federal election campaigns. They have an extensive network of partners and resources to prepare political campaigns with the resources they need to stay secure. In partnership with Yubico, they provide YubiKeys at no cost to political organizations and campaigns.

yubico

About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based passkey authentication security at scale to customers in over 160 countries.

For more information, please visit: www.yubico.com.