VETO THESE ELECTION SCAMS

As the 2024 voting cycle approaches, crooks see an opportunity to steal

BY **SARI HARRAR**

It's a big election year—and criminals are already out in force with scams aimed at stealing your cash and personal information while making you think you're taking part in the democratic process. Barbara from Michigan told the AARP Fraud Watch Network Helpline she lost $500 to an impostor claiming to be President Joe Biden's press secretary, who texted her repeatedly for donations via gift cards. Desi from Florida paid $20,000 to a social media impostor for Donald Trump memorabilia and had to cancel his credit cards to protect his finances. Mary from California is trying to stop repeat credit card charges to a political campaign.

Law enforcement and election officials across the U.S. are warning about voter registration scams, criminals deploying artificial intelligence to impersonate candidates on the phone and social media, and schemes to garner campaign contributions and interfere with voting. Another danger: fake political surveys designed to steal personal data, including credit card account information.

Election-related scams often target older adults, simply because they're so politically engaged. "Almost half of individual campaign contributions come from people age 50 and older," says Brett G. Kappel, a Washington-based campaign finance lawyer.

The months before a presidential election are a boom time for crooks. "Politics brings out passion in people, which is always an opportunity to steal," says AJ Nash, vice president at the cybersecurity company ZeroFox.

Here's the scoop on three big election year consumer scams—and how to avoid them:

▶SCAM PACS AND BOGUS DONATIONS

Sounding like charities, scammers register as political action committees (PACs) with the Federal Election Commission. By phone, email, text and social media, they solicit donations they say will support candidates and campaigns that promote worthy causes—from breast cancer awareness to firefighters. Instead, they keep most of the money for themselves, Kappel says. The haul can be huge: One large group of "scam PACs" raked in more than $140 million over the previous two election cycles, according to a 2023 investigation of FEC records of PACs by the news website *The Daily Beast*.

Donation-seeking scammers may impersonate candidates, campaigns and political interest groups, sometimes using AI—riding on the sense of election urgency to push you to act, says Melanie McGovern, of the International Association of Better Business Bureaus. **Outsmart them:** Never donate right away to groups that contact you, Kappel says. Give directly to candidates and campaigns by looking up their contact information online. You can review a PAC's finances by looking the group up on the FEC's website at fec.gov/data. And check how groups accept payment. "Legitimate PACs must have bank accounts and will accept credit cards," Kappel says. "Scammers want you to use PayPal, send a check or, worse yet, a gift card, because the money can't be recovered."

▶FRAUDULENT SURVEYS

Pollsters measure public opinion through surveys by email, text, social media and phone. Scam surveys aim to steal your personal identifying information, often by offering a gift or other incentive that requires you to provide your credit card number, Social Security number, address or date of birth, the Pennsylvania attorney general's office warns. **Outsmart them:** Don't assume phone surveys must be legit if you're on the National Do Not Call Registry—these types of calls are exempt, according to the Federal Trade Commission. A legit political poll won't offer you a gift or ask for personal information, says Amy Nofziger, AARP's director of fraud victim support. "I do not participate in phone surveys," she says. "You can't verify who they really are."

▶VOTER REGISTRATION SCAMS

Early in the 2024 primary election season, officials in some states were already warning about voter registration scams that use phone calls and text messages to phish for personal information. Voters are asked to confirm their registration by clicking on a link. Scammers may impersonate election officials and ask you to provide personal data to update or renew your registration, the National Association of Secretaries of State warns.

Criminals exploit confusion about registration rules, which vary by state. "The dates aren't as clear as when your taxes are due," notes Michael Kaiser, president and CEO of Defending Digital Campaigns. **Outsmart them:** You can't register to vote by phone and you can't vote online in a federal election. But voting rules vary from state to state, and so do deadlines for mail-in and absentee ballots. In many cases, regulations have changed since 2020. Cut through the confusion "by going to the secretary of state or board of elections for your state," Kaiser says. Don't click on a link in an email or text. Find trustworthy information about your state's rules at aarp.org/electionguides. ■

***Sari Harrar is a contributing editor** for AARP who frequently writes about fraud for the* AARP Bulletin.

***Have questions related to scams?** Call the AARP Fraud Watch Network Helpline toll-free at **877-908-3360**. For the latest fraud news and advice, go to **aarp.org/fraudwatchnetwork**.*

CHRIS GASH