



SECUREFI INTELLIGENCE BRIEF

Election Edition

Election Scams and Deception

What is happening now, what history tells us, and what to watch next

NONPARTISAN

October 2026

Edited by David Haberland and Stephen Partello

Published by SecureFi, Inc.

Executive Summary

Election-related deception is not new.

What is changing is the speed, realism and reach of the technology used to deliver it.

In October 2026, federal authorities warned about:

- suspicious mailings targeting election-related organizations
- fraudulent voter-registration messages
- threats against election workers
- cyber activity targeting election and campaign officials
- election-themed fundraising and merchandise scams
- AI-assisted impersonation

These threats follow patterns seen in previous elections, including fake social-media identities, false voting instructions, threatening emails, misleading robocalls, AI-generated voices, fabricated government videos and hoax threats.

The underlying method is remarkably consistent:

Create trust or fear. Create urgency. Make the target act before independently verifying what is real.

This brief separates specific **documented events** from **SecureFi assessment** so readers can distinguish what authorities say is happening now from patterns SecureFi believes are worth watching in the days ahead.

This brief is nonpartisan. SecureFi does not advocate for or against any candidate, political party or political position.

Key Judgment

The signals people traditionally used to establish trust are becoming easier to fake.

A familiar voice is no longer proof.

Caller ID is not proof.

A government name or insignia is not proof.

A professional-looking website is not proof.

A social-media profile is not proof.

Even a message from a real account may not be trustworthy if that account has been compromised.

The protective question increasingly has to change from:

“Does this look real?”

to:

“Can I independently verify that it is real?”

What Is Happening Now in 2026

1. Suspicious letters are targeting election-related organizations

Since mid-October, a nationwide campaign of suspicious mailings has targeted election-related offices, elected officials and other organizations.

Reporting based on briefings with election officials indicated that **more than 100 letters** had been sent nationwide, although not all were directed specifically to election offices.

By October 20, election offices in **at least 32 states** had reportedly been affected, along with more than three dozen members of Congress from both parties.

Some letters contained white powder or another unidentified substance.

On October 23, the FBI and U.S. Postal Inspection Service confirmed that they were investigating suspicious letters sent to recipients including:

- elected officials
- Secretaries of State and election offices
- other election-related organizations
- media organizations
- public and private polling companies

At the time of the FBI alert, no hazardous material had been identified, although laboratory testing was continuing.

Why it matters

A threat does not have to cause physical harm to have an effect.

It can force evacuations, disrupt government operations, consume law-enforcement resources and create an opening for misinformation about what happened.

If you see a claim that an election office or polling location has been affected, verify it through the responsible election authority or law enforcement before sharing it.

2. Fake voter-registration messages

The FBI is warning about fraudulent texts and emails claiming there is a problem with a person's voter registration.

A message might look like this:

VOTER ALERT

Your voter registration could not be verified.

Confirm your information before Election Day.

votercheck-now[.]example

The link may lead to a site designed to resemble an official election page and collect personal information.

Red flags

- an unexpected registration problem
- an urgent deadline
- a link supplied by the sender
- a request to verify personal information
- a website reached through an unsolicited text or email

Before you act

Do not use the supplied link.

Start independently with **Vote.gov** or your official state or local election authority.

3. Threats against election workers

On October 15, the FBI warned about threats directed toward election workers.

The FBI's definition includes officials, staff, volunteers, contractors, vendors and others involved in election administration.

Threats can arrive through telephone calls, email, social media or in-person communications.

Why it matters to everyone

A real threat can quickly create a second problem: inaccurate information about what the threat means.

Posts may claim:

- an election office has closed
- voting has stopped
- workers have evacuated
- ballots were compromised
- a polling location is unsafe

Some reports may be accurate. Others may be outdated, mistaken or deliberately fabricated.

Verify the event before sharing conclusions about it.

4. Cyber actors are targeting election and campaign officials

On October 16, the FBI and CISA warned about malicious cyber activity targeting election officials, candidates and political organizations.

The agencies highlighted techniques including:

- phishing
- smishing
- credential theft
- attempts to obtain sensitive information

A compromised legitimate account can then create an additional risk.

A message can come from a real account and still be fraudulent.

The account identity is one trust signal. It is not final proof that a particular message or request is legitimate.

5. Fraudsters are using the election to target money and information

The FBI has identified several election-themed fraud schemes.

Fake political committees

Fraudsters can create organizations that resemble legitimate political committees and solicit donations.

Before donating, independently research the organization and check political committees through **FEC.gov** where applicable.

“Campaign investment pools”

Scammers may claim money placed into a political campaign pool will produce a guaranteed return if a particular candidate wins.

Political contributions are not investments.

Political merchandise scams

Fraudulent sellers may advertise political merchandise, collect payment and never deliver it.

Treat an unfamiliar political site like any unfamiliar online retailer: independently check the seller before providing payment information.

What History Tells Us

Previous elections demonstrate how quickly the method can change while the underlying deception stays the same.

2016: Fake Americans online

The Justice Department alleged that Russian actors created fictitious American identities and social-media accounts, purchased advertisements and communicated with real Americans while hiding the operation’s origin.

Lesson: A profile that appears local or familiar does not establish who actually controls it.

2016: “Vote by text”

Deceptive social-media images falsely suggested people could vote by text. At least **4,900 unique telephone numbers** texted the number used in the campaign images.

Lesson: Unusual voting instructions should be verified through an election authority.

2020: False robocall warnings

Prerecorded calls falsely warned voters of consequences associated with voting by mail. The FCC ultimately imposed a **\$5.1 million forfeiture**.

Lesson: Fear and urgency are reasons to verify, not reasons to act immediately.

2020: Threatening emails under a false identity

Tens of thousands of voters received threatening messages falsely presented as coming from a domestic political organization. The Justice Department later charged two Iranian nationals.

Lesson: The displayed sender is not proof of who sent a message.

2024: AI-generated voice

Before New Hampshire’s presidential primary, voters received robocalls using an AI-generated imitation of President Biden’s voice and spoofed caller ID. The FCC later imposed a **\$6 million penalty**.

A New Hampshire jury later acquitted the consultant of separate state voter-suppression and impersonation charges in June 2025.

Lesson: A familiar voice is no longer proof.

2024: Fabricated government content and hoax threats

The FBI warned about fabricated election-related videos falsely claiming to come from the Bureau and, on Election Day, bomb threats involving polling locations that had not been determined to be credible.

Lesson: Government branding and dramatic claims should be independently verified.

SECUREFI ASSESSMENT

What to Watch for in the Final Week and Immediately After Election Day

The following is **SecureFi's assessment** based on documented tactics from previous election cycles together with FBI and CISA warnings issued in October 2026.

These are **not claims that each tactic is currently occurring everywhere.**

They are patterns worth recognizing because they have been used previously, resemble current warnings or take advantage of conditions that exist around a fast-moving election.

1. Claims that voting information or requirements changed

Messages may claim:

- a polling location moved
- voting hours changed
- a location closed
- a new identification or other voting requirement applies
- a voting method is no longer available

Election requirements can legitimately change.

SecureFi assessment

Do not assume a claimed change is either true or false because of how the message looks.

Verify it directly with your state or local election authority.

2. Fake registration emergencies

Messages may claim your registration was cancelled, incomplete or requires immediate verification.

The objective could be identity theft, collection of personal information or discouraging participation.

SecureFi assessment

A message that creates an urgent problem and then conveniently supplies the solution deserves additional scrutiny.

Move outside the message and verify independently.

3. AI-generated voices, video and statements

The 2024 election demonstrated that AI-generated voices can be used in election communications.

Fabricated videos have also falsely claimed to come from government agencies.

SecureFi assessment

Audio or video that looks convincing should no longer be treated as authentication by itself.

Verify important announcements through the person, organization, agency or election authority supposedly responsible for them.

4. Hoax threats and false reports of disruption

Past elections have included hoax threats involving polling locations, and the suspicious-letter investigation shows disruptive threats remain a current concern.

SecureFi assessment

Separate the incident from the claims surrounding it.

A genuine suspicious package does not prove claims about:

- who sent it
- why it was sent
- whether voting was affected
- whether ballots were damaged
- whether incidents are coordinated

Wait for responsible authorities to establish what is known.

5. Fabricated fraud or system-compromise claims

Previous elections have included false or fabricated claims involving hacked voter data, compromised election systems and fake government investigations.

SecureFi assessment

Technical language, screenshots, leaked-looking data or government branding can make an unsupported claim appear authoritative.

Ask one question:

Who independently confirms this?

If the answer is no one, treat the claim as unverified.

6. Fraud immediately after Election Day

Election-related fraud can continue after voting ends.

Periods involving recounts, litigation, breaking news and uncertainty can create opportunities for:

- fake fundraising
- bogus legal-defense appeals
- false recount solicitations
- fabricated government notices
- fake investigations
- malicious breaking-news links
- cryptocurrency or payment requests

Legitimate campaigns, political committees and parties may also continue raising money after an election.

A post-election fundraising request is not itself evidence of fraud.

Verify the organization independently and use **FEC.gov** where applicable before giving.

SecureFi assessment

Political emotion can create the same vulnerability as fear or financial urgency.

Before sending money, providing information or sharing a dramatic claim, verify who is actually asking and where the information originated.

What to Do

Pause.

Urgency, fear, anger and excitement can all reduce the time people spend checking information.

Move outside the message.

Do not automatically use the supplied link, telephone number, QR code or reply button.

Verify independently.

Use an election authority, government agency or organization you located yourself.

For dramatic claims, ask:

Who independently confirms this?

Preserve evidence.

Keep screenshots, messages, sender addresses, telephone numbers, URLs, voicemail, audio, video and payment information.

Report when appropriate.

Reporting can help authorities connect incidents, identify patterns and warn others.

Where to Check and Report

If you need to...	Use
Check registration or official voting information	Vote.gov or your state/local election authority
Check a political committee before donating	FEC.gov

Report an election-related scam involving money or personal information

IC3.gov

Report election-worker threats, intimidation or suspected election crimes

FBI, your local field office, **Tips.FBI.gov** or **1-800-CALL-FBI**

Report an illegal or spoofed robocall or text

FCC consumer complaint system

Report a state voting problem

Your **state or local election authority** or appropriate state agency

Report an immediate threat to life or safety

911

The SecureFi Takeaway

The technology has changed significantly.

The core deception has not.

Fraud and influence operations still depend on someone believing the sender is real, the authority is genuine or the request must be acted on immediately.

AI makes more of those signals easier to reproduce.

The protective habit remains straightforward:

Pause. Verify independently. Check before you act.

SecureFi.AI helps people evaluate suspicious messages, calls, links, payment requests and situations before acting.

When something has already gone wrong, SecureFi helps people preserve evidence, understand reporting options and work through recovery steps.

Received something suspicious? Check it on SecureFi.AI.

Already affected? Preserve the evidence and get help with reporting and recovery.

Sources

Federal Bureau of Investigation / U.S. Postal Inspection Service

October 23, 2026

Suspicious Letters Containing White Powder Mailed to State and Local Election Officials, Media Organizations, and Public and Private Polling Companies

Used for:

- the nationwide suspicious-letter investigation
- recipient categories
- FBI and U.S. Postal Inspection Service involvement
- hazardous-material testing status
- suspicious-mail safety guidance

Votebeat

October 15, 2026

Used for:

- early reporting on the nationwide suspicious-mail campaign
- reporting that officials had been briefed about more than 100 letters
- operational impact of the mailings

Axios

October 20, 2026

Used for:

- reporting that election offices in at least 32 states had been affected
- congressional offices receiving suspicious mail
- broader scale of the mailing campaign

Federal Bureau of Investigation / Internet Crime Complaint Center

October 15, 2026

Scammers Exploit 2026 U.S. Midterm Election to Perpetrate Multiple Fraud Schemes

Used for:

- fraudulent voter-registration messages
- campaign investment-pool schemes
- ScamPACs
- political merchandise scams
- AI-assisted impersonation
- election-scam reporting guidance

Federal Bureau of Investigation / Internet Crime Complaint Center

October 15, 2026

FBI Cautions About Threats to Election Workers Ahead of the November 2026 Midterm Election

Used for:

- definition of election workers
- threats directed toward election workers
- communication channels used for threats
- reporting guidance

Federal Bureau of Investigation / Cybersecurity and Infrastructure Security Agency

October 16, 2026

Cyber Threat Actors Use a Variety of Techniques to Target Election and Campaign Officials

Used for:

- phishing and smishing
- credential theft
- targeting of election officials, candidates and political organizations
- attempts to obtain sensitive information

Federal Bureau of Investigation / Internet Crime Complaint Center

October 15, 2026

FBI Warns Voters on Election Crimes Ahead of the November 2026 Midterm Election

Used for:

- election crimes affecting voters
- voter suppression and intimidation
- election-crime reporting guidance

U.S. Department of Justice

February 16, 2018

Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System

Used for:

- Internet Research Agency activities
- fictitious U.S. identities
- concealed foreign activity
- social-media influence operations during the 2016 election cycle

U.S. Department of Justice

2021 to 2023

Douglass Mackey election-interference case

Used for:

- deceptive “vote by text” campaign
- at least 4,900 unique telephone numbers responding to the deceptive messages
- federal prosecution and conviction

The conviction was overturned on appeal in 2025.

Federal Communications Commission

2021 and 2023

Burkman/Wohl robocall enforcement actions

Used for:

- 2020 mail-voting robocalls
- false claims involving warrants, debt collection and CDC vaccine tracking
- 1,141 unlawful prerecorded calls
- \$5,134,500 forfeiture

U.S. Department of Justice

November 18, 2021

Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election

Used for:

- threatening emails
- false sender identity
- attempted election-related cyber activity
- fabricated election-related video

Federal Communications Commission

September 26, 2024

FCC Fines Man Behind Election Interference Scheme \$6 Million for Illegal Deepfake Robocalls

Used for:

- AI-generated imitation of President Biden
- caller-ID spoofing
- New Hampshire primary robocalls
- \$6 million FCC penalty

A New Hampshire jury later acquitted the consultant of separate state voter-suppression and impersonation charges in June 2025.

FBI and CISA

September 2024

Used for:

- warnings concerning false claims involving compromised voter-registration data
- the distinction between publicly available voter information and evidence of a successful cyberattack

Federal Bureau of Investigation

November 2, 2024

FBI Statement on Election-Security-Related Videos Falsely Claiming to Be from the Bureau

Used for:

- fabricated videos falsely presented as FBI communications
- false election-security claims

Federal Bureau of Investigation

November 5, 2024

FBI Statement on Bomb Threats to Polling Locations

Used for:

- bomb threats involving polling locations in several states
- FBI statement that none had been determined to be credible at that time
- public reporting guidance

About This Intelligence Brief

SecureFi Intelligence Briefs examine significant fraud, cyber, consumer and personal-risk developments using authoritative sources, documented historical patterns and clearly labeled analysis.

This **Election Edition** is nonpartisan and does not advocate for or against any candidate, political party or political position.

Documented events and government warnings are presented separately from SecureFi assessments.

SecureFi assessments identify patterns or risks that may warrant attention based on the information available at publication. They should not be interpreted as claims that a particular event occurred unless the brief specifically identifies it as documented.

SecureFi reviews each cited source and translates published information into practical risk guidance. SecureFi does not independently investigate the underlying events and does not replace election authorities, law enforcement or other responsible organizations.

Information is provided for education and risk awareness.

Election procedures, registration status, polling locations and other voting questions should always be verified directly with the appropriate official election authority.

Edited by David Haberland and Stephen Partello
Published by SecureFi, Inc.
October 2026