Public Service Announcement

FBI & CISA

Alert Number: I-081424-PSA

September 12, 2024

Just So You Know: False Claims of Hacked Voter Information Likely Intended to Sow Distrust of U.S. Elections

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness of attempts to undermine public confidence in the security of U.S. election infrastructure through the spread of disinformation falsely claiming that cyberattacks compromised U.S. voter registration databases.

Malicious actors continue to spread false or misleading information in an attempt to manipulate public opinion and undermine confidence in U.S. democratic institutions. One of the most common tactics involves using obtained voter registration information as evidence to support false claims that a cyber operation compromised election infrastructure. The reality is that having access to voter registration data is not by itself an indicator of a voter registration database compromise. Most U.S. voter information can be purchased or otherwise legitimately acquired through publicly available sources. In recent election cycles, when cyber actors have obtained voter registration information, the acquisition of this data did not impact the voting process or election results.

As of this publication, the FBI and CISA have no information suggesting any cyberattack on U.S. election infrastructure has prevented an election from occurring, changed voter registration information, prevented an eligible voter from casting a ballot, compromised the integrity of any ballots cast, or disrupted the ability to count votes or transmit unofficial election results in a timely manner.
The FBI and CISA urge the American public to critically evaluate claims of “hacked” or “leaked” voter information and to remember that most voter registration information is available to the public.

Public Recommendations:

- Do not accept claims of intrusion at face value and remember that these claims may be meant to influence public opinion and undermine the American people’s confidence in our democratic process.
- Be cautious of social media posts, unsolicited emails from unfamiliar email addresses, or phone calls or text messages from unknown phone numbers that make suspicious claims about the elections process or its security.
- If you have questions about election security and/or administration in your jurisdiction, rely on state and local government election officials as your trusted sources for election information.
- Visit your state and local elections office websites for accurate information about the elections process. Many of these offices have websites that use a “.gov” domain, indicating they are an official government site.

Role of the FBI and CISA in Elections

The FBI and CISA coordinate closely with federal, state, local, and territorial election officials to provide services and information to help election officials further secure election processes and maintain the resilience of U.S. elections.

The FBI is responsible for investigating and prosecuting election crimes, foreign malign influence operations, and malicious cyber activity targeting election infrastructure.

CISA, as the as the Sector Risk Management Agency for the Election Infrastructure subsector, helps critical infrastructure owners and operators, including those in the election community, safeguard the security and resilience of election infrastructure from physical, cyber, and operational security threats.

Victim Reporting and Additional Information

The FBI and CISA encourage the public to report information concerning suspicious or criminal activity, such as ransomware attacks, to the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov. Cyber incidents can also be reported to CISA by calling 1-844-Say-CISA (1-844-729-2472), mailing report@dhs.cisa.gov, or reporting online at cisa.gov/report.

For additional assistance, to include common terms and best practices, please visit:

- Stop Ransomware | CISA for additional resources to tackle ransomware more effectively.
- CISA #Protect2024 for additional resources to protect against the cyber, physical, and operational security risks to election infrastructure.
- Protected Voices for additional resources to protect against online foreign influence operations, cyber threats, and federal election crimes.