Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters

October 02, 2020 (2020-10-02T11:30:00-04:00)

Alert Number

I-100220-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

The FBI and CISA are issuing this PSA as a part of a series on threats to the 2020 election to enable the American public to be prepared, patient, and participating voters.

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to help the public recognize and avoid spoofed election-related internet domains and email accounts during the 2020 election year.

Spoofed domains and email accounts are leveraged by foreign actors and cybercriminals and can be easily mistaken for legitimate websites or emails. Adversaries can use spoofed domains and email accounts to disseminate false information; gather valid usernames, passwords, and email addresses; collect personally identifiable information; and spread malware, leading to further compromises and potential financial losses.

Cyber actors set up spoofed domains with slightly altered characteristics of legitimate domains. A spoofed domain may feature an alternate spelling of a word (**"electon"** instead of **"election"**), or use an alternative top-level domain, such as a **"[.]com"** version of a legitimate **"[.] gov"** website. Members of the public could unknowingly visit spoofed domains

while seeking information regarding the 2020 election. Additionally, cyber actors may use a seemingly legitimate email account to entice the public into clicking on malicious files or links.

The FBI and CISA urge all members of the American public to critically evaluate the websites they visit and the emails sent to their personal and business email accounts, to seek out reliable and verified information on election information.

Recommendations

- Verify the spelling of web addresses, websites, and email addresses that look trustworthy but may be close imitations of legitimate election websites.
- Seek out information from trustworthy sources, verifying who produced the content and considering their intent. The Election Assistance Commission (https://www.eac.gov) provides a vast amount of verified information and resources.
- Ensure operating systems and applications are updated to the most current versions.
- Update anti-malware and anti-virus software and conduct regular network scans.
- Do not enable macros on documents downloaded from an email unless absolutely necessary, and only then, after ensuring the file is not malicious.
- Disable or remove unneeded software applications.
- Use strong two-factor authentication if possible, via biometrics, hardware tokens, or authentication apps.
- Do not open e-mails or attachments from unknown individuals. Do not communicate with unsolicited e-mail senders.
- Never provide personal information of any sort via e-mail. Be aware that many e-mails requesting your personal information appear to be legitimate.

The FBI is responsible for investigating and prosecuting election crimes, malign foreign influence operations, and malicious cyber activity targeting election infrastructure and other U.S. democratic institutions. CISA helps critical infrastructure owners and operators, including those in the election community, remain resilient against physical and cyber threats. The FBI and CISA provide services and information to uphold the security, integrity, and resiliency of U.S. electoral processes.

Victim Reporting and Additional Information

The FBI encourages the public to report information concerning suspicious or criminal activity to their local field office (www.fbi.gov/contact-us/field-offices) or to the FBI's Internet Crime Complaint Center (www.ic3.gov). For additional assistance, best practices, and common terms, please visit the following websites:

- Protected Voices: www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices
- Election Crimes and Security: www.fbi.gov/scams-and-safety/common-scams-and-crimes/election-crimes-and-security
- #Protect2020: www.cisa.gov/protect2020