

FBI warns of digital ‘spoofing’ scams during election

October 31, 2020



Just one week away from election day, The FBI has some tips on dealing with how bad actors can use “spoofing” to try to impact your vote.

Foreign actors and cybercriminals use spoofed domains and email accounts to appear legitimate. Through them, the bad actors can 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, i.e., “electon” instead of “election”, or use “[.]com” in place of “[.] gov.”

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 urges all Americans to critically evaluate the websites they visit and the emails sent to their personal and business email accounts and to seek out reliable and verified information on the election.

Here are some other recommendations:

Verify the spelling of web addresses and email addresses that look trustworthy but may, in reality, just be close imitations of legitimate election websites.

Seek out information from trustworthy sources, verifying who produced the content and considering their intent. One option: the Election Assistance Commission at <https://www.eac.gov>. That group 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.

Use strong two-factor authentication if possible, via biometrics (such as face or fingerprint scans), 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.

The FBI is responsible for investigating malign foreign influence operations and malicious cyber activity targeting election infrastructure and other U.S. democratic institutions.

Report potential federal election crimes to the FBI. In California, contact the Roseville office at (916) 746-7000 or submit a tip online at tips.fbi.gov.

Finally – learn more about how you can protect your vote with the FBI's Protected Voices campaign. You can find more resources at www.fbi.gov/protectedvoices or www.fbi.gov/elections.