SECURING CYBER INFRASTRUCTURE: POLITICAL CAMPAIGNS

Cyber incidents affecting political campaigns are becoming far more complex and can have dire consequences. Use the recommended strategies below to help protect your campaign against malicious activity.

IMPLEMENT MULTI FACTOR AUTHENTICATION (MFA)

MFA is a layered approach to security for online accounts, applications, and data. It requires a user to present a combination of two or more authenticators to verify their identity for login. Ensure MFA is turned on for campaign email, social media, financial, and any other campaign-related electronic accounts, applications, or services.

- For more information on MFA, reference CISA's More than a Password website at https://www.cisa.gov/MFA.

USE STRONG PASSWORDS

Simple passwords, or common identifying information, like birthdays, are not safe for protecting important accounts. Go beyond easy-to-guess passwords and reduce the risk of password hacking by:

- Using password managers to generate and secure passwords to protect your environment from unverified users.
- Requiring long, random, unique passwords for each account to beat automated software attacks.
- For more information on strong password creation, reference CISA's Use Strong Passwords website at https://www.cisa.gov/secure-our-world/use-strong-passwords.

UPDATE SOFTWARE PROMPTLY

Software updates are issued to fix security risks. Keeping software up to date is an easy way to stay safer.

- Watch for notifications, install updates as soon as possible, and turn on automatic updates, where possible.
- For more information on updating software, reference CISA's Update Software webpage at https://www.cisa.gov/secure-our-world/update-software.

ENCRYPT MESSAGING AND SYSTEMS

For sensitive communications, use encrypted messaging services to provide an additional layer of protection. Using end-to-end encryption helps secure the privacy of your communication.

SECURE CAMPAIGN AND PERSONAL DEVICES

Candidate's family members are often targets for hackers looking for an entry point to access sensitive campaign information and data, as their devices may be less secure than the candidate's own devices.

- Ensure campaign and personal devices for staff AND family members are accounted for and kept secure.
- At a minimum, all personal devices and accounts should be up to date and use strong passwords and MFA.

RECOGNIZE AND REPORT PHISHING

Phishing is a common tactic where users are "baited" to open harmful links, emails, or attachments that request our sensitive information or download malicious software. Messages are often designed to look like they came from a trusted source.

- Educate campaign staff on how these tactics work and conduct phishing test for staff to practice identification and reporting. Phishing should be reported to https://www.cisa.gov/report or to report@cisa.gov.

CREATE A CYBER INCIDENT RESPONSE PLAN

Even with implementing all recommended good practices, incidents may still occur. Creating and practicing an organizational incident response plan will help all team members understand, prepare for, and mitigate the risks of potential cyber incidents. For more information on creating an incident response plan, reference CISA's Incident Response Planning Guide at https://www.cisa.gov/resources-tools/resources/cyber-incident-guide.

- Create a cyber incident response plan that team members are aware of and trained on response procedures.
- Report cyber incidents to CISA at https://www.cisa.gov/report by emailing **report@cisa.gov** or (888) 282-0870.