Homeland Security

# Campaign Checklist | Securing Your Cyber Infrastructure

Political campaigns are facing cyber-attacks of varied sophistication. The Department of Homeland Security (DHS) has created this cybersecurity checklist to assist your campaign in protecting against malicious actors. This is not an exhaustive list, as good security requires constant attention based upon evolving risk. Implementing these protocols, and instilling a culture of digital vigilance, will put your team in the best position to focus on your campaign priorities instead of the consequences of a cyber incident.

## USE TWO-FACTOR AUTHENTICATION (2FA)

- Two-factor authentication allows an extra layer of security for email, social media, and database accounts by requiring users to provide a second login beyond the user's password.

## IMPLEMENT STRONG PASSWORD PRACTICES

- Use password managers to secure all of your passwords. Password managers allow you to manage all your accounts in one place. Make sure to review a password manager before selecting.
- Use a long password to access the password manager. We recommend using a unique string of words that can be easily remembered, but difficult to guess.
- Use different passwords for all accounts, including email and social media.

## ENABLE AUTO-UPDATE TO INSTALL SECURITY PATCHES IN A TIMELY MANNER

- Once patches are available, quickly install onto the operating systems of your computers, mobile devices, and databases. Unpatched systems pose unnecessary risks to your systems.

## USE ENCRYPTED MESSAGING APPS OR SYSTEMS WHEN NECESSARY

- For sensitive communications, use encrypted messaging services to provide an additional layer of protection.
- Secure messaging apps are available for download. Users should research a messaging app before using.

## HAVE A PLAN TO QUICKLY RESPOND TO CYBER INCIDENTS

- Despite following these practices, cyber incidents may occur. Have a plan in place to respond and know which authorities to contact depending on the type and severity of the incident.
- Report cyber incidents to DHS by contacting nccicustomerservice@hq.dhs.gov or 888-282-0870.
- For more information on creating an incident response plan, visit https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf

## SECURE CAMPAIGN AND PERSONAL DEVICES

- Ensure all campaign and personal devices for staff **AND** family members are accounted for and kept secure.
- Candidates and their family members are potential targets of actors looking to gain access to their devices and the information they contain. Candidates should ensure all family members secure their personal devices.
- At a minimum, all personal devices, personal email accounts, and personal social media accounts should utilize strong passwords and two-factor authentication.

## BEWARE OF PHISHING ATTEMPTS

- Phishing is a common attack where emails, texts, or other communication are sent to entice a user to provide their username and password, open an attachment that has destructive software hidden in it, or click a link that directs them to a website containing malicious software.
- Protect yourself from phishing attacks:
  - If the content of a message seems unusual or out of the norm for the sender, or it is from a sender you do not recognize, do not open an attachment or click a link until you have contacted the sender.
  - Do not click on links for emails in your junk folder, even if they appear legitimate.
  - Take a second to review links and attachments before opening.
  - If you suspect a text or email to be a phishing attempt, report it to the appropriate IT provider.

---

If you are experiencing or suspect malicious cyber behavior, contact the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870 or NCCICCustomerService@hq.dhs.gov.