PROTECTED VOICES

VIDEO SERIES HIGHLIGHTS

Below is a summary of the FBI's recommendations for strengthening your political campaign's cybersecurity, arranged by the titles of the videos released as part of the FBI's Protected Voices initiative. Use this summary as a starting point for researching and deploying security measures that are the best fit for your campaign.

Social Engineering

Cyber attacks often begin with a social engineering technique such as phishing, so train your campaign staffers to recognize and thwart these types of attacks.

Patching, Firewalls, and Anti-Virus Software

Keep your systems patched, ideally with automatic updates; set effective rules for your firewalls; and install anti-virus software with regular or automatic updates.

Passwords

Require your staffers' passwords to be long; encourage the use of a passphrase rather than a password. Also consider using a password keeper/vault, setting up logging on your network to track password activity, and adding multi-factor authentication.

Information Security (InfoSec)

Educate everyone involved in your campaign on good InfoSec practices, create a written InfoSec policy, and develop and implement ongoing training/testing for InfoSec policy compliance.

Browser and App Safety

Web browsers are how your devices access the Internet, so adjust your browser settings—and the settings on your mobile devices—to maximize your privacy and security.

Safer Campaign Communications

Communications can include your personal email, your official email, messaging apps, and social media posts. To secure these channels, use encryption, disable archiving, use access controls, disable remote wiping, use account lockout, and patch your systems.

Wi-Fi

When using open/public Wi-Fi, access the Wi-Fi via a virtual private network (VPN). Only visit Internet sites that use HTTPS, don't let your device automatically connect to available networks, and turn off your device's Wi-Fi connections when you don't need to use them. Don't do your banking and shopping transactions on open/public Wi-Fi.

Continued

Router Hardening

To protect your router—which is the gateway between your network and the Internet—change your router's default password, apply patches regularly or automatically, choose your network name carefully, and use WPA2 for encryption.

Cloud-Based Services

Cloud-based services may offer your campaign increased cybersecurity measures, so research reputable cloud services vendors with the best balance of privacy, security, and cost for you.

Virtual Private Networks

A VPN—which creates a secure tunnel for your data to transit the Internet using a network of private servers—is a great way for your campaign to keep its communications and Internet activities more private, especially when using public Wi-Fi or other points of access not under your direct control.

Have You Been Hacked?

By the time you realize your system is compromised, all of your data may already have been taken. There are a number of red flags to look for that might indicate a cyber attack, including passwords not working, a large number of pop-up ads, unexplained online activity, slow-running devices, and altered system settings.

Incident Response

Develop a cyber incident response team and plan so your campaign is prepared for a potential cyber incident. Your plan should include the three components of an incident response team: technical, legal, and managerial. Identify a backup way for your team to communicate without relying on your computer network (no email, texts, or VOIP communications that use your campaign's network).

your voice matters

so protect it

fbi.gov/protectedvoices