The FBI's Protected Voices initiative provides tools and resources to political campaigns, companies, and individuals to protect against online foreign influence operations and cybersecurity threats.

Protected Voices includes information and guidance from the FBI, the Department of Homeland Security, and the Director of National Intelligence.

The Threat: Foreign adversaries, including Russia and China, and foreign-aligned groups try to illegally influence American political processes. Three common foreign influence methods are:

Cyberattacks against political campaigns and government infrastructure	Secret funding or influence operations to help or harm a person or cause	Disinformation campaigns on social media platforms that confuse, trick, or upset the public
These attacks might include adversaries hacking and leaking sensitive information from computers, databases, networks, phones, and emails.	Tactics include political advertising from foreign groups pretending to be U.S. citizens, lobbying by unregistered foreign agents, and illegal campaign contributions from foreign adversaries.	For example, a foreign group may purposefully spread false or inconsistent information about an existing social issue to provoke all sides and encourage conflict.

The Defense: Protect your voice. The Protected Voices webpage (fbi.gov/protectedvoices) offers videos, printable materials, and other resources for political campaigns, companies, and individuals to use as action plans and training aids. Learn about foreign influence tactics and simple ways to protect your digital devices, social media accounts, and private information.

We encourage U.S. citizens working in critical infrastructure sectors to join InfraGard (infragard.org), an FBI-sponsored public-private partnership that offers the latest intelligence bulletins on cybersecurity and other threats.

Report: Election officials and campaign staff should report suspicious activity to their local FBI field office (fbi.gov/contact-us/field-offices)

fbi.gov/protectedvoices

Protected Voices Video Quick Guide

Find full content videos at fbi.gov/protectedvoices

- **Director's Message:** An introduction to Protected Voices by FBI Director Christopher Wray.
- **Browser and App Safety:** Adjust your Internet and app settings to maximize your privacy and security.
- **Business Email Compromise:** Defend your business email accounts to keep an adversary from impersonating you.
- **Cloud-Based Services:** Research reputable cloud services vendors with the best balance of privacy, security, and cost for you.
- **Foreign Influence:** Russia, China, Iran, and other foreign countries try to influence the U.S. political process and provoke social conflicts.
- **Have You Been Hacked?** By the time you realize your system is compromised, all of your data may already have been taken.
- **Incident Response:** Develop a cyber incident response team so your campaign is prepared for a potential cyber incident.
- **Information Security (InfoSec):** Educate everyone involved in your campaign on good InfoSec practices.
- **Passphrases and Multi-Factor Authentication:** Passwords should be long passphrases, consider using password keeper programs, and require the use of multi-factor authentication.
- **Patching, Firewalls, and Anti-Virus Software:** Keep your systems patched, ideally with automatic updates.
- **Ransomware:** Train staff in cyber hygiene, limit users' access to network files they actually need, and back up your data to a standalone source.
- **Router Hardening:** Change your router's default password, apply patches regularly or automatically, choose your network name carefully, and use at least WPA2 for encryption.
- **Safer Campaign Communications:** Use encryption, disable archiving, use access controls, disable remote wiping, use account lockout, and patch your systems.
- **Social Engineering:** Cyberattacks often begin with a social engineering technique, such as phishing.
- **Social Media Literacy:** Keep a healthy skepticism—consider why something might have been posted online, and who stands to gain from that information.
- **Supply Chain:** Look into the apps, services, and technology you use to identify who's really providing a service
- **Virtual Private Networks:** A VPN is a great way for your campaign to keep its communications and Internet activities more private, especially when using public Wi-Fi.
- **Wi-Fi:** When using open/public Wi-Fi, access it via a VPN. Only visit Internet sites that use HTTPS, and don't let your device automatically connect to available networks.

fbi.gov/protectedvoices

October 2019