La iniciativa del FBI *Protected Voices* [Voces protegidas] ofrece herramientas y recursos para campañas políticas, empresas y personas para que se protejan de operaciones de influencia extranjera en el internet y de amenazas a la ciberseguridad.

El FBI, el Departamento de Seguridad Nacional y el Director de Inteligencia Nacional ofrecen información y orientación a través de *Protected Voices.*

La amenaza: Los adversarios extranjeros, que incluyen a Rusia y a China, y grupos aliados a países extranjeros intentan influenciar de forma ilícita los procesos políticos estadounidenses. Los tres métodos comunes de la influencia extranjera son:

Los ciberataques contra las campañas políticas y la infraestructura gubernamental	**El financiamiento secreto o los operativos con influencia para ayudar o perjudicar a una persona o a una causa**	**Las campañas de desinformación en plataformas de medios sociales que confunden, engañan o trastornan al público**
Estos ataques podrían incluir a adversarios que logran acceso de forma ilícita a información confidencial en computadoras, bases de datos, redes, teléfonos y correos electrónicos que después la divulgan.	Las tácticas incluyen la publicidad política de grupos extranjeros que fingen ser ciudadanos estadounidenses, el cabildeo por agentes extranjeros no registrados y las contribuciones ilegales a campañas por adversarios extranjeros.	Por ejemplo, un grupo extranjero puede difundir deliberadamente información falsa o incoherente sobre una cuestión social existente para provocar a todas las partes y fomentar el conflicto.

Defensa: proteja su voz. La página web de *Protected Voices* (fbi.gov/protectedvoices) proporciona videos, materiales que se pueden imprimir y otros recursos para campañas políticas, empresas y personas para que los utilicen en planes de acción y en materiales educativos. Conozca las tácticas de la influencia extranjera y las maneras simples de proteger sus dispositivos digitales, sus cuentas de medios sociales y su información privada.

Instamos a los ciudadanos estadounidenses que trabajan en los sectores de la infraestructura crítica a que se unan a InfraGard (infragard.org) —una alianza público-privada patrocinada por el FBI que brinda los boletines de inteligencia más recientes sobre la ciberseguridad y otras amenazas—.

Dé parte: Los funcionarios electorales y el personal de la campaña deben dar parte de actividades sospechosas a su oficina local del FBI. (fbi.gov/contact-us/field-offices)

fbi.gov/protectedvoices

Guía rápida para los videos de *Protected Voices*

Encuentre los videos con contenido completo en fbi.gov/protectedvoices

- **Mensaje del director:** Introducción a *Protected Voices* por el director del FBI, Christopher Wray.
- **Seguridad en navegadores y aplicaciones:** Configure su internet y sus aplicaciones para maximizar su privacidad y seguridad.
- **Fraude empresarial por correo electrónico (BEC, por sus siglas en inglés):** Defienda sus cuentas de correo electrónico para evitar que un adversario se haga pasar por usted.
- **Servicios en la nube:** Busque proveedores acreditados de servicios en la nube que le brinden el mejor equilibrio en lo que toca a privacidad, seguridad y costo.
- **Influencia extranjera:** Rusia, China, Irán y otros países extranjeros intentan influenciar el proceso político de Estados Unidos y provocar conflictos sociales.
- **¿Ha sido atacado(a)?** Para cuando se dé cuenta de que su sistema ha sido vulnerado, es posible que ya le hayan robado todos sus datos.
- **Respuesta a incidentes:** Elabore un equipo de respuesta a incidentes cibernéticos para que su campaña esté preparada para un posible incidente cibernético.
- **Seguridad de la información:** Eduque a toda persona que participe en su campaña sobre las buenas prácticas referentes a la seguridad de la información.
- **Frases de contraseña y autentificación de factores múltiples:** Las contraseñas deben ser frases largas. Considere el uso de programas de control de contraseñas y requiera que se use la autentificación de factores múltiples.
- **Programas de parches, cortafuegos y antivirus:** Mantenga parches en sus sistemas, preferiblemente con actualizaciones automáticas.
- **Ransomware:** Capacite al personal en ciberhigiene. Limite el acceso de los usuarios a los archivos en la red que realmente necesiten y haga una copia de seguridad de sus datos en una fuente independiente.
- **Endurecimiento del enrutador:** Cambie la contraseña predeterminada de su enrutador, aplique parches de forma regular o automática, elija el nombre para su red cuidadosamente y utilice al menos el protocolo WPA2 para la codificación.
- **Comunicaciones más seguras para una campaña:** Codifique, deshabilite el archivado, utilice los controles de acceso, deshabilite la posibilidad de borrar remotamente, utilice el bloqueo de cuentas y aplique parches a sus sistemas.
- **Ingeniería social:** Los ciberataques a menudo comienzan con una técnica de ingeniería social, como la suplantación de la identidad.
- **Alfabetización de los medios sociales:** Mantenga un escepticismo saludable. Considere por qué algo pudo haber sido publicado en internet y quién se beneficiará de esa información.
- **Cadena de suministro:** Analice las aplicaciones, los servicios y la tecnología que usted emplea para identificar quién realmente está proporcionando un servicio.
- **Redes privadas virtuales (VPN, por sus siglas en inglés):** Una VPN es una buena manera de hacer que su campaña mantenga las comunicaciones y actividades de internet más privadas, especialmente cuando usa el acceso Wi-Fi público.
- **Acceso Wi-Fi:** Al utilizar el acceso Wi-Fi público o accesible, hágalo a través de una VPN. Solo visite sitios de internet que utilicen el protocolo HTTPS y no permita que su dispositivo se conecte automáticamente a las redes disponibles.

fbi.gov/protectedvoices

Octubre de 2019