GUÍA DE PREVENCIÓN Y RESPUESTA AL SWATTING PARA TRABAJADORES ELECTORALES Y ORGANISMOS DE SEGURIDAD

DESCRIPCIÓN

Swatting (Anglicismo por 'falsa alarma') es un término utilizado para describir la actividad delictiva por parte de un individuo o un grupo que deliberadamente proporciona información falsa a los organismos de seguridad al denunciar falsamente la existencia de una amenaza grave en un lugar en particular con el fin de que dichos organismos de seguridad respondan con unidades tácticas, o lo que comúnmente se conoce como un equipo SWAT, una unidad élite para armas y tácticas especializadas. Esta peligrosa práctica pone en riesgo a la persona o ubicación objetivo y a los organismos de seguridad y utiliza recursos críticos de respuesta inmediata para emergencias reales. A finales del 2023 y principios del 2024, hubo múltiples incidentes de *swatting* dirigidos específicamente a los trabajadores electorales[1]. Este documento de orientación proporciona una descripción general del *swatting* y las prácticas recomendadas para prevenir y responder a incidentes de *swatting* tanto para trabajadores electorales como para organismos de seguridad.

ENTENDER EL SWATTING

Los actores tanto domésticos como extranjeros utilizan el *swatting* como un método para acosar o intimidar a personas y empresas, tales como funcionarios del gobierno de los Estados Unidos, instituciones religiosas, escuelas, periodistas, ejecutivos de empresas y celebridades. También pueden tratar de interrumpir las operaciones de infraestructura crítica, inducir miedo o caos, distraer a los organismos de seguridad de otros delitos o emergencias, o simplemente ganar atención o notoriedad. Al igual que las tácticas de *doxing* y *phishing*, los actores maliciosos que participan en el *swatting* a menudo se basan en información de código abierto o técnicas de ingeniería social para descubrir información acerca del blanco de sus acciones. Los "*swatters*" llaman a las líneas de emergencia como el 9-1-1 o a las líneas que no sean para emergencia de las agencias de seguridad y denuncian una situación de emergencia violenta falsa que requiere una respuesta inmediata, como un tirador activo, una amenaza de bomba, un allanamiento de morada o una situación de rehenes, tratando de reunir una respuesta de emergencia a la mayor escala posible. Incluso pueden usar tecnología para que parezca que la llamada de emergencia proviene del número de teléfono de la víctima[2]. Los "*swatters*" a menudo presentan un escenario plausible y a veces, incluyen información personal adquirida en línea sobre la víctima para hacer que la llamada sea más creíble.

Trágicamente la confusión por parte de los blancos de dichas acciones como de los oficiales de los equipos de respuesta ha tenido consecuencias fatales. El *swatting* también desvía los limitados recursos de respuesta a emergencias reales, causando indirectamente daños a las víctimas más allá de los objetivos específicos.

REDUCIR EL RIESGO PARA LOS TRABAJADORES Y LAS INSTALACIONES ELECTORALES

Aunque hasta la fecha los incidentes de *swatting* han sido dirigido a los hogares de los funcionarios electorales, los actores maliciosos podrían ampliar esta táctica para atacar otras instalaciones, con el fin de interrumpir las operaciones electorales. Esto podría incluir intentos de *swatting* para interrumpir las operaciones electorales en los lugares de votación, las oficinas electorales o las instalaciones centrales de escrutinio. Los organismos de seguridad y los trabajadores electorales pueden tomar medidas para reducir los riesgos de *swatting*. Para ayudar a prevenir posibles incidentes de *swatting*, los funcionarios electorales deben **estar en contacto con los organismos de seguridad pública locales y los servicios de emergencia** para compartir, según la política de privacidad de su organización, los nombres y direcciones de los trabajadores electorales y los lugares relacionados con las elecciones, y colaborar en estrategias de mitigación. También se urge a los trabajadores electorales a implementar prácticas óptimas para **reducir la disponibilidad de su información de identificación personal en línea**[3].

[1] " "Election Officials' homes 'swatted' as presidential race heats up." https://www.cnn.com/2024/03/13/politics/*swatting*-election-officials-invs/index.html

[2] Suplantación de identidad de llamadas | Comisión Federal de Comunicaciones (fcc.gov)

[3] CISA Insights: Mitigación de los impactos del doxing en infraestructuras críticas | CISA

Prevención de *Swatting*: Qué Hacer para Mitigar el Riesgo de un Incidente de *Swatting*

- **Establezca relaciones entre las oficinas electorales, los organismos de seguridad pública y los servicios de emergencia.**
  - Los organismos de seguridad deben considerar ponerse en contacto con sus trabajadores electorales locales para entender sus preocupaciones y necesidades.
  - Igualmente, los trabajadores electorales deben considerar trabajar con los socorristas locales para conocer sus procedimientos operativos estándar para distintos tipos de llamadas de emergencia.
  - Los organismos de seguridad pública y los trabajadores electorales locales deben considerar discutir los procedimientos para establecer una alerta local para su lugar de residencia y de votación en su sistema local de despacho asistido por computadora (CAD, por sus siglas en inglés). La alerta local en CAD le informará al personal policial que responda llamando a un número de teléfono proporcionado para avisarles del despacho antes de que la policía llegue al lugar y alertar al personal del 9-1-1 y a los posibles oficiales que respondan con un mensaje específico para inquietudes acerca del *swatting*.

- **Comparta información crítica sobre las instalaciones electorales con los socorristas.** Las oficinas electorales deben considerar compartir la siguiente información con los organismos de seguridad y otras entidades para manejo de emergencias y asegurarse de entender la importancia de mantener su confidencialidad:
  - Las direcciones de los lugares electorales específicos, incluyendo los lugares de votación, las instalaciones de almacenamiento de la infraestructura electoral y del sistema de votación, las oficinas administrativas y las instalaciones centrales de escrutinio;
  - Información crítica de las instalaciones para dichas ubicaciones, como planos de planta e información acerca de incendios y servicios públicos; e
  - Información de contacto del personal electoral crítico quien puede ser contactado en caso de un posible incidente.

- **Establezca protocolos de comunicación y entrenamiento para posibles escenarios.** Las oficinas electorales y los organismos de seguridad público deben considerar:
  - Discutir y ejercitar posibles escenarios de *swatting* entre las partes interesadas para que todas las partes entiendan la posible respuesta con antelación.
  - Establecer canales de comunicación con el personal electoral local, regional y estatal para compartir información sobre incidentes de *swatting*, de modo que, si el incidente ocurre en una jurisdicción, se alerte a otras acerca de la posibilidad de incidentes similares.
  - Proporcionar a los trabajadores electorales y a quienes trabajan en las urnas, entrenamiento acerca del *swatting* y de desescalación.
  - Dar capacitación en ciberseguridad a todo el personal para reforzar las buenas prácticas individuales en torno a la protección de la información de identificación personal en línea.
  - Recomendar a los trabajadores electorales que hablen sobre el riesgo de *swatting* con otros miembros de su hogar; planeen y practiquen qué hacer en caso de un incidente de *swatting* en su residencia.

- **Manténgase informado sobre las tendencias de amenazas nacionales.** Los organismos de seguridad deben tener en cuenta:
  - Consultar con otras autoridades locales, estatales y federales, incluida la Oficina Federal de Investigaciones (FBI) y el Departamento de Seguridad Nacional (DHS), sobre las tendencias actuales en el *swatting*, así como los indicadores de llamadas de *swatting*.
  - Proporcionar capacitación al personal, incluidos los despachadores del 9-1-1, sobre los indicadores de *swatting* y el potencial de *swatting* en relación con las elecciones.

- **Reduzca la disponibilidad de información de identificación personal de los trabajadores electorales en línea**. Los trabajadores electorales deben tener en cuenta lo siguiente:
  - Verificar si la ley estatal permite que los registros de los empleados públicos sean omitidos de las bases de datos de búsqueda en línea y optar por este servicio, de estar disponible.
  - Usar servicios que eliminan información de identificación personal en internet.
  - Utilizar contraseñas seguras y únicas en todos los dispositivos y cuentas, incluyendo los dispositivos domésticos inteligentes.
  - Activar la autenticación multifactorial (MFA) en todos los dispositivos y cuentas, incluyendo los dispositivos domésticos inteligentes.
  - Usar una red privada virtual (VPN, por sus siglas en inglés) para ocultar las direcciones IP de los dispositivos y, por lo tanto, la ubicación física asociada.
  - Estar al tanto de lo que se publica en las redes sociales referente a la ubicación de las personas.

Respuesta a incidentes de *swatting*: Qué hacer durante y después de un incidente de *swatting*

Recomendaciones para los trabajadores electorales sobre qué hacer durante un incidente de *swatting*: En el desafortunado caso de que su hogar o lugar de trabajo sea blanco de un ataque de *swatting*, mantenga la calma. Escuche y coopere con los organismos de seguridad. Si bien es posible que no sea una emergencia real, es probable que los organismos de seguridad no estén al tanto de esto y envíen una gran respuesta policial a su ubicación. Las siguientes son algunas consideraciones para ayudar a mitigar el riesgo durante la respuesta de los servicios de emergencia a un incidente de *swatting*:

- Durante una respuesta policial, es posible que lo traten como sospechoso hasta que el incidente sea resuelto. La prioridad de los organismos de seguridad es garantizar que no haya ninguna amenaza. Es probable que la situación sea muy estresante y frustrante tanto para usted como para los servicios de emergencia. Para resolver la situación rápidamente, cumpla con todas las órdenes de los organismos de seguridad, no ofrezca ninguna resistencia y responda las preguntas de manera concisa. Para garantizar su seguridad, asegúrese de que sus manos estén visibles para los organismos de seguridad y muévase de manera lenta y deliberada.
- Si sospecha haber sido objeto de un incidente de *swatting*, llame al 9-1-1. Dele al despachador su nombre, dirección y cuantos detalles le sea posible. Infórmele que no hay una emergencia en su hogar u oficina (según corresponda) y esté preparado para responder cualquier pregunta.
- Es posible que los organismos de seguridad no permitan que nadie salga de las instalaciones hasta que ellos hayan establecido que no es una emergencia real. Los funcionarios electorales deben asegurarse de que su Plan para Continuidad de Operaciones incluya cómo continuarán las operaciones en caso de un incidente de *swatting* en una oficina u otra locación electoral, por ejemplo, asegurándose de que los equipos y materiales críticos estén seguros.

Recomendaciones para los trabajadores electorales y los organismos de seguridad después de un incidente de *swatting*: Si ocurre un incidente de *swatting*, las siguientes recomendaciones ayudarán a facilitar la adecuada denuncia del incidente y ayudarán a identificar el riesgo potencial para otras oficinas y trabajadores electorales.

- Si los trabajadores electorales creen que ellos, su familia, su personal o su oficina han sido víctimas de un incidente de *swatting*, primero deben denunciar este posible delito a la policía local y luego comunicarse con el FBI a través de los Coordinadores de Delitos Electorales en su oficina local, enviar una pista al 1-800-CALL-FBI (1-800-225-5324) o en línea en tips.fbi.gov[4].
- Si ocurre un incidente de *swatting* dirigido a trabajadores o instalaciones electorales, anime al personal electoral estatal a compartir información sobre el incidente, para que otras jurisdicciones electorales sean alertadas sobre la posibilidad de incidentes similares. Después del incidente, los trabajadores electorales pueden notificar a CISA al report@cisa.gov o al 1-844-Say-CISA (1-844-729-2472) para que pueda alertar a otros trabajadores electorales en caso de un evento a mayor escala.
- Los incidentes de *swatting* pueden ser eventos locales o parte de una acción más amplia a nivel nacional. Los organismos de seguridad deben considerar la posibilidad de denunciar inmediatamente estos incidentes a su oficina local del FBI.
- Los organismos de seguridad federales, estatales y locales pueden ponerse en contacto con el Grupo de Rastreo de la Industria (ITG, por sus siglas en inglés) para ayudar a determinar la identidad del originador de la llamada o del proveedor de la puerta de enlace. El ITG actualmente sirve como el consorcio de rastreo designado por la Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) en virtud de la Ley federal TRACED de 2019, y las regulaciones vigentes de la FCC requieren que todos los proveedores de servicios de voz nacionales cooperen con el proceso de rastreo.[5] A través del proceso de rastreo, el ITG obtiene información sobre las personas que llaman infractoras, así como sobre los proveedores de servicios de voz que transportan, originan e introducen tráfico ilegal en los Estados Unidos. El ITG obtiene rutinariamente esta información dentro de uno o dos días, incluso horas luego de iniciar un rastreo, y el proceso funciona incluso si la llamada es falsificada. Los organismos de seguridad pueden iniciar solicitudes de asistencia al ITG en: https://tracebacks.org/for-government. Es importante tener en cuenta que, debido a las diferentes políticas de retención de datos entre los proveedores de telecomunicaciones, la eficacia de este servicio disminuye con el tiempo, y recomendamos iniciar las solicitudes de rastreo lo antes posible.

RECURSOS ADICIONALES

- Comité para Elecciones Seguras y Protegidas: "Combatting Swatting Attempts ". https://safeelections.org/wp-content/uploads/2024/01/Combatting-*Swatting*-Attempts-CSSE-.pdf

[4] Election Crimes and Security - FBI
[5] About – Industry Traceback Group (tracebacks.org)