ORIENTACIÓN DE PREVENCIÓN Y RESPUESTA CONTRA EL SWATTING PARA LOS TRABAJADORES ELECTORALES Y LA POLICÍA

DESCRIPCIÓN GENERAL

El "swatting" es un término utilizado para describir la actividad delictiva de un individuo o grupo que, a sabiendas, comunica información falsa a la policía en la que se sugiere que existe una amenaza grave en un lugar determinado para que esta responda con unidades tácticas, o lo que comúnmente se conoce como equipo de tácticas y armas especiales (SWAT, por sus siglas en inglés). Esta táctica peligrosa pone en riesgo a la persona o al lugar objetivo y a la policía, y quita recursos esenciales del personal de respuesta para las emergencias reales. A finales de 2023 y principios de 2024, se produjeron múltiples incidentes de swatting específicamente dirigidos a trabajadores electorales[1]. Este documento de orientación ofrece una descripción general del swatting y las prácticas recomendadas para prevenir estos incidentes y responder a ellos, tanto para los trabajadores electorales como para la policía.

¿QUÉ ES EL SWATTING?

Agentes tanto extranjeros como nacionales utilizan el swatting como método para acosar o intimidar a individuos y empresas, como funcionarios del Gobierno estadounidense, instituciones religiosas, escuelas, periodistas, ejecutivos de empresas y celebridades. También es posible que pretendan interrumpir las operaciones de la infraestructura crítica, causar miedo o caos, desviar la atención de la policía de otros delitos o emergencias, o simplemente llamar la atención o adquirir notoriedad. De forma similar a las tácticas de doxeo y suplantación de identidad, los agentes maliciosos que se dedican al swatting a menudo utilizan información de código abierto o técnicas de ingeniería social para descubrir información sobre su objetivo. Los agentes llaman a líneas de emergencia, como el 9-1-1, o a líneas para situaciones que no son emergencias de las agencias policiales e informan sobre situaciones falsas de emergencia violentas que requieren una respuesta inmediata, como un tirador activo, una amenaza de bomba, un allanamiento de morada o una situación con rehenes, en un intento de reunir la mayor respuesta de emergencia posible. Incluso pueden utilizar tecnología para que parezca que la llamada de emergencia procede del número de teléfono de la víctima[2]. Los agentes suelen presentar un escenario convincente y, a veces, incluyen información personal recopilada en Internet sobre la víctima para que la llamada resulte más creíble.

La confusión de los objetivos y del personal de respuesta ha tenido trágicas consecuencias mortales. El swatting también desvía los limitados recursos de respuesta de emergencia de las situaciones de emergencia reales, lo que indirectamente perjudica a las víctimas aparte de a los objetivos específicos.

CÓMO REDUCIR EL RIESGO PARA LOS TRABAJADORES Y LAS INSTALACIONES ELECTORALES

Aunque, hasta el momento, los incidentes de swatting han tenido como objetivo los domicilios de los funcionarios electorales, los agentes maliciosos podrían ampliar esta táctica para atacar a otras instalaciones con el objetivo 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 recuento. La policía y los trabajadores electorales pueden tomar medidas para reducir los riesgos del swatting. Para ayudar a prevenir posibles incidentes de swatting, los funcionarios electorales deben **colaborar con la policía y los equipos de respuesta a emergencias locales** para compartir, de acuerdo con la política de privacidad de su organización, los nombres y domicilios de los trabajadores electorales y los lugares relacionados con las elecciones, y colaborar en las estrategias de mitigación. También se recomienda a los trabajadores electorales que apliquen las prácticas recomendadas 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 Caller ID Spoofing | Federal Communications Commission (fcc.gov)

3 CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure | CISA

Prevención del swatting: qué hacer para mitigar el riesgo de un incidente de swatting

- **Establecer relaciones entre las oficinas electorales, la policía y los servicios de emergencia.**
  - La policía debería considerar ponerse en contacto con los trabajadores electorales locales para comprender sus inquietudes y necesidades.
  - Asimismo, los trabajadores electorales deberían considerar la posibilidad de trabajar con el personal de respuesta local para conocer sus procedimientos operativos estándar ante distintos tipos de llamadas de emergencia.
  - La policía y los trabajadores electorales locales deben considerar la posibilidad de analizar los procedimientos para establecer una bandera o alerta para su domicilio y los lugares de votación en el sistema de despacho asistido por computadora (CAD, por sus siglas en inglés) local. Las alertas o banderas en el CAD informarán al personal policial que responda para que llame a un número de teléfono indicado a fin de alertar a los miembros del despacho antes de la llegada de los agentes policiales al lugar y alertar al personal del 9-1-1 y a los posibles cuerpos que respondan con un aviso específico acerca de los problemas relacionados con el swatting.

- **Compartir información esencial sobre las instalaciones electorales con el personal de respuesta.** El personal de las oficinas electorales debe considerar la posibilidad de compartir la siguiente información con la policía y otros socios de gestión de emergencias, y garantizar que conocen la importancia de mantener su confidencialidad:
  - Las direcciones de los lugares específicos de las elecciones, incluidos 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 recuento.
  - Información fundamental sobre estas instalaciones, como planos e información sobre los servicios públicos y contra incendios.
  - Información de contacto del personal electoral fundamental con el que se puede comunicar en caso de un posible incidente.

- **Establecer protocolos de comunicación y capacitar para posibles escenarios.** Las oficinas electorales y la policía deberían considerar lo siguiente:
  - Debatir y ensayar posibles escenarios de swatting entre las partes interesadas clave para que todas las partes entiendan con antelación cómo podría ser la respuesta.
  - Establecer canales de comunicación con el personal electoral local, regional y estatal para compartir información sobre incidentes de swatting de tal forma que, si el incidente ocurre en una jurisdicción, se alerte a las demás sobre la posibilidad de que se produzcan incidentes similares en la suya.
  - Impartir a los trabajadores electorales y a los miembros de los centros de votación capacitación sobre el swatting y las técnicas de desescalada.
  - Impartir capacitación en ciberseguridad a todo el personal para reforzar las prácticas recomendadas individuales sobre protección de la información de identificación personal en línea.
  - Recomendar a los trabajadores electorales que analicen el riesgo del swatting con otros miembros de su hogar, que planifiquen y practiquen lo que deben hacer en caso de que se produzca un incidente de swatting en su domicilio personal.

- **Mantenerse informado sobre las tendencias nacionales de amenazas.** La policía debería considerar lo siguiente:
  - Consultar a otras autoridades locales, estatales y federales, incluida la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) y el Departamento de Seguridad Nacional (DHS, por sus siglas en inglés), sobre las tendencias actuales en swatting, además de los indicadores de llamadas de este tipo de incidentes.
  - Impartir capacitación al personal, incluidos los despachadores del 9-1-1, sobre los indicadores y la probabilidad de casos de swatting en relación con las elecciones.

- **Reducir la disponibilidad de la información de identificación personal en línea de los trabajadores electorales.** Los trabajadores electorales deberían considerar lo siguiente:
  - Comprobar si las leyes estatales permiten omitir los expedientes de los empleados públicos de las bases de datos de búsqueda en línea y, si es posible, elegir este servicio.

- Utilizar servicios que eliminan la información de identificación personal de Internet.
- Utilizar contraseñas seguras y únicas en todos los dispositivos y las cuentas, incluso en los dispositivos domésticos inteligentes.
- Activar la autenticación multifactor (MFA, por sus siglas en inglés) en todos los dispositivos y las cuentas, incluso en los dispositivos domésticos inteligentes.
- Utilizar una red privada virtual (VPN, por sus siglas en inglés) para ocultar las direcciones de protocolo de Internet (IP, por sus siglas en inglés) de los dispositivos y, por tanto, la ubicación física correspondiente.
- Ser consciente de lo que se publica en las redes sociales en relación con la ubicación de las personas.

Respuesta a incidentes de swatting: qué hacer durante un incidente de swatting y después de este

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 objetivo de un ataque de swatting, mantenga la calma. Escuche a la policía y coopere con ella. Aunque es posible que no haya una emergencia real, probablemente la policía no lo sepa y acuda a su ubicación con una presencia policial considerable. A continuación, se detallan algunas consideraciones para ayudar a mitigar el riesgo en caso de que los servicios de emergencia respondan a un incidente de swatting:

- Durante una respuesta de la policía, es posible que lo traten como a un sospechoso hasta que se resuelva el incidente. La prioridad de la policía es asegurarse de que no haya ninguna amenaza. Probablemente, la situación resulte muy estresante y frustrante tanto para usted como para el personal de los servicios de emergencia. Para resolver la situación con rapidez, cumpla todas las órdenes de la policía, no se resista y responda a las preguntas de forma concisa. Para velar por su seguridad, asegúrese de que sus manos estén siempre a la vista de la policía y muévase de manera lenta y deliberada.
- Si sospecha que podría haber sido el objetivo de un incidente de swatting, llame al 9-1-1. Indique al despachador su nombre, domicilio y la mayor cantidad de información posible. Comuníquele que no hay ninguna emergencia en su domicilio u oficina (según corresponda) y esté preparado para responder a cualquier pregunta que pudiera hacerle.
- Es probable que la policía no permita que nadie abandone las instalaciones hasta que haya comprobado que no se trata de una emergencia real. Los funcionarios electorales deben asegurarse de que su Plan de Continuidad de Operaciones incluya cómo se desarrollarán las operaciones en caso de un incidente de swatting en una oficina electoral u otro lugar de votación, por ejemplo, asegurándose de que los equipos y materiales críticos estén seguros.

Recomendaciones para los trabajadores electorales y la policía tras un incidente de swatting: Si se produce este tipo de incidente, las siguientes acciones recomendadas ayudarán a facilitar la notificación adecuada y a identificar posibles riesgos para otras oficinas y trabajadores electorales.

- Si los trabajadores electorales creen que ellos mismos, 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, ponerse en contacto con la FBI a través de los coordinadores de delitos electorales de su oficina local y enviar un aviso al 1-800-CALL-FBI (1-800-225-5324) o en línea en tips.fbi.gov[4].
- Si se produce un incidente de swatting dirigido contra trabajadores o instalaciones electorales, se recomienda al personal electoral estatal que comparta la información sobre el incidente, con el fin de alertar a otras jurisdicciones electorales sobre la posibilidad de que se produzcan incidentes similares. Después del incidente, los trabajadores electorales pueden notificar a la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) enviando un correo electrónico a report@cisa.gov o llamando al 1-844-Say-CISA (1-844-729-2472) para que pueda alertar a otros trabajadores electorales en caso de que el incidente se produzca a mayor escala.
- Los incidentes de swatting pueden ser de carácter local o formar parte de una acción de alcance nacional. La policía debería considerar la posibilidad de informar estos incidentes inmediatamente a su oficina local de la FBI.

[4] Election Crimes and Security — FBI

- La policía federal, estatal y local puede ponerse en contacto con el Grupo de Seguimiento del Sector (ITG, por sus siglas en inglés) para que le ayude a determinar la identidad del emisor de la llamada o del proveedor de la puerta de enlace. El ITG actualmente funciona como el consorcio de seguimiento designado por la Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) conforme a la Ley de Sanción Penal y Disuación del Abuso de Llamadas Telefónicas Robotizadas (TRACED, por sus siglas en inglés) de 2019, y las regulaciones de la FCC actualmente requieren que todos los proveedores de servicios de voz nacionales cooperen con el proceso de seguimiento.[5] A través del proceso de seguimiento, el ITG obtiene información sobre las personas que llaman infractoras, además de los proveedores de servicios de voz que transportan, originan y traen tráfico ilegal a los Estados Unidos. De manera habitual, el ITG obtiene esta información dentro de uno o dos días, si no horas, después de iniciar un seguimiento, y el proceso funciona incluso si una llamada es falsificada. La policía puede iniciar solicitudes de asistencia del 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 transcurso del tiempo, y recomendamos iniciar solicitudes de seguimiento lo antes posible.

RECURSOS ADICIONALES

- Comité para Elecciones Seguras y Protegidas (Committee for Safe and Secure Elections): “Cómo combatir los intentos de swatting”. https://safeelections.org/wp-content/uploads/2024/01/Combatting-Swatting-Attempts-CSSE-.pdf

[5] About – Industry Traceback Group (tracebacks.org)