NOTA DE ACTUALIDAD 10/2018

12 de julio de 2018

Carolina San Juan López[*]

Fortificando la seguridad en las redes y la seguridad de la Información

Nota de actualidad 10: Fortificando la seguridad en las redes y la seguridad de la Información. Protección contra la desinformación online (Las "fake news" o noticias falsas)

El presente texto es una síntesis del documento Strengthening network & Information Security & Protecting against online disinformation ("Fake News")

La Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), responsable de este documento, es un centro de seguridad de red y de información especializada para la Unión Europea, sus estados miembros, el sector privado y los ciudadanos de la Unión Europea. ENISA trabaja con estos grupos para desarrollar recomendaciones y consejos para el buen uso de la seguridad de información.

Más información sobre ENISA: *www.enisa.europa.eu*

1. INTRODUCCIÓN

Recientemente, las «fake news» o noticias falsas han recibido mucha atención mediática por interrumpir potencialmente los procesos democráticos de manera global. Es necesario iniciar un diálogo en la Unión Europea para tratar las posibles respuestas a este fenómeno[1].

En este sentido, el uso inapropiado de: un ordenador conectado a Internet, una cuenta online comprometida, una cuenta online falsa o plataformas online podrían considerarse como armas cuando publicar en las redes sociales, mandar correos electrónicos, mandar *spams* (correos electrónicos no deseados con fines publicitarios) y realizar otras actividades en línea pueden causar daños a otras personas, así como a la sociedad a largo plazo.

Los recientes acontecimientos sugieren que la difusión de la desinformación online está resultando ser una amenaza en crecimiento para el funcionamiento efectivo del proceso democrático. Este hecho ha sido demostrado en las elecciones presidenciales de 2016 de Estados Unidos, cuando, en una encuesta realizada en diciembre de 2016, el 64% de los entrevistados afirmaron que las «fake news» causaron una gran confusión respecto a los hechos básicos de los acontecimientos contemporáneos. Las acusaciones posteriores de intromisión cibernética en las elecciones, en el contexto de la Unión Europea publicadas en los medios, incluyen las elecciones presidenciales francesas y el referéndum sobre la participación de Reino Unido en la Unión Europea.

[1] En este contexto, «desinformación online» se define como: información online o en línea falsa, imprecisa o errónea diseñada, publicada y promovida para fines malos o inadecuados.

[*] Alumna en prácticas de la Universidad Pontificia de Comillas

Un factor clave en la difusión de la desinformación online es el comportamiento humano. Se ha demostrado que las noticias falsas consiguen llamar más la atención que aquellas que son verdaderas. Además, estas noticias falsas se difunden más que las verdaderas, lo que manipula la opinión pública.

2. CONSIDERACIONES: DE DESINFORMACIÓN ESPECÍFICA A DESINFORMACIÓN ONLINE

2.1. La inteligencia artificial y la desinformación online

Las técnicas y métodos de la inteligencia artificial pueden ser desde una decisión simple, haciendo algoritmos, hasta un reconocimiento de patrones y exploración de datos.

En la era digital, la información se difunde por todas partes del mundo en cuestión de segundos y la revisión manual de los hechos no es una solución ni efectiva ni eficiente de acabar con la desinformación online. Lo que se está intentando ahora es que la inteligencia artificial sea capaz de separar las noticias verdaderas de las noticias falsas. Esto sería posible a través del reconocimiento de patrones. La desinformación online puede ser identificada a partir de señales de artículos etiquetados como falsos por personas tiempo atrás.

Mientras que esta tecnología sigue en desarrollo, los resultados de este análisis deben ser validados por seres humanos. Las fuentes necesarias deben ser puestas en marcha por los operadores de las plataformas online importantes para asegurar la precisión y la coordinación de este asunto.

2.2. Desincentivos económicos

También deben considerarse los impulsores económicos utilizados para la difusión de la desinformación online. Una estrategia de los desincentivos económicos podría incluir los recortes en la publicidad de sitios que están creados para difundir la desinformación online.

3. CONSIDERACIONES EN LA RED GENERAL Y EN LA SEGURIDAD DE INFORMACIÓN

3.1. Control de la contraseña

Como se ha mencionado en líneas anteriores, las cuentas en línea comprometidas pueden ser consideradas como un arma que puede causar daños. Para conservar la integridad de la cuenta y prevenir la suplantación de personalidad es necesario contar con una contraseña segura.

Además, para acceder a todas las plataformas online se recomienda:

- Que los algoritmos estén diseñados para indicar al usuario que debe emplear una contraseña segura (contraseñas largas con caracteres especiales).
- El uso de la autentificación de la contraseña, que proporciona un nivel independiente adicional de información.
- Que sea necesario cambiar de contraseña periódicamente, por ejemplo, cada tres meses.

Estas medidas deberían ayudar significativamente a reducir el número de cuentas en línea comprometidas que pueden causar daños.

3.2. Sistemas de elección e infraestructuras calificados como críticos

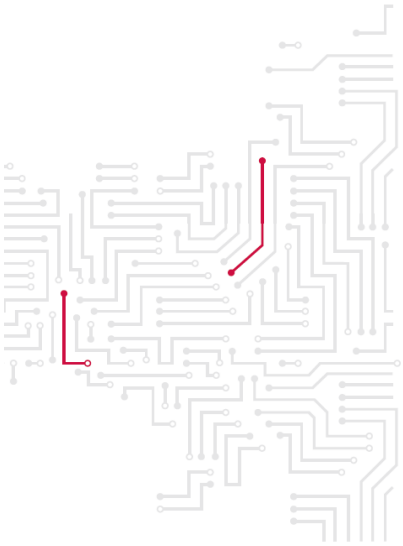
Hace poco se ha declarado que las elecciones políticas de la Unión Europea han sido perjudicadas por la difusión de la desinformación online. Esta amenaza interfiere, potencialmente, en el proceso democrático de la Unión Europea.

Reconocer el comportamiento humano y las acciones, a menudo, necesarias para que el usuario proteja su contraseña, hará que los operadores de las plataformas online desempeñen un papel activo en este proceso.

La Unión Europea no es la única que está sufriendo esta amenaza. Varios Estados Miembro ya han actuado para identificar y mitigar los riesgos asociados con la desinformación online. Es más, en la Unión Europea, un gran número de países ya se han informado sobre el tema y han buscado soluciones.

3.3. Privacidad y protección de datos

Tener una Regulación General de Protección de Datos (GDPR) habría prevenido los patrones de procesamiento de datos personales que han sido revelados, recientemente, en los medios de comunicación.



Medidas de seguridad razonables y las tecnologías de mejora de la privacidad (PETs), tales como el uso de la minimización de datos, la confidencialidad y los credenciales designados, deberían ser desarrolladas por los operadores de las plataformas en línea.

4. RECOMENDACIONES

4.1. Recomendaciones de desinformación específica a desinformación online

a. Inteligencia artificial

Deberían emplearse algoritmos para ayudar a las campañas de detección de la desinformación en línea y el mal uso de las plataformas en línea como la publicidad no deseada. Estos algoritmos deben ser verificados por seres humanos antes de que se realice alguna acción.

b. Reputación online y transparencia

Las plataformas online deben considerar los resultados de sus análisis de desinformación y proponer una manera transparente de construir la confianza de los usuarios.

c. Desincentivos económicos

Se debe desarrollar una estrategia para crear desincentivos económicos, como los recortes en publicidad de sitios creados para expandir la desinformación online.

d. Verificación de la fuente

Los operadores de los medios online deben crear firmas que luego sean incluidas en los artículos nuevos, para que los usuarios puedan verificar el contenido de la fuente.

e. Opciones de información online

Las plataformas online deberían identificar la posible desinformación online e informar de ello. Esta información debería ser examinada por los operadores para determinar la acción adecuada.

4.2. Recomendaciones de seguridad de red y de información

a. Requisitos mínimos obligatorios para las contraseñas

Para el acceso a todas las plataformas online se recomienda:

-que los algoritmos sean utilizados para indicar a los usuarios que deben poseer una contraseña segura.

-el uso de una segunda autentificación de la contraseña.

-que sea obligatorio cambiar contraseñas de manera periódica, por ejemplo, cada tres meses.

b. Sistemas de elección, procesos e infraestructuras clasificados como críticos

La obligación legal debe ser considerada para clasificar los sistemas de elección, los procesos y las infraestructuras como críticos, para asegurar que están siendo operadas con un nivel alto de red y con seguridad de información en sus sistemas, procesos e infraestructuras.

c. Obligación de seguridad en la red y de seguridad de información para las organizaciones políticas

Una obligación legal debería ser que las organizaciones políticas utilicen un nivel alto de red y una seguridad de información en sus sistemas, procesos e infraestructuras.

d. Cumplimiento de los requisitos de protección de datos

Las medidas de seguridad razonables y las tecnologías para mejorar la privacidad (PETs), como el uso de la minimización de los datos, la discreción o los credenciales designados, deben ser emplea dos por los operadores de las plataformas online.