Red Europea de Prevención de la Delincuencia

Serie de toolboxes de la REPD

Nº. 13

Prevención del fraude individual

Resumen ejecutivo

La 13ª toolbox de la serie publicada por la Secretaría de la REPD se centra en la prevención del *fraude individual*. La Presidencia búlgara (primer semestre de 2018) decidió centrarse en:

«[…] *cuestiones relacionadas con el fraude, en particular las estafas telefónicas. Este tipo de delito se ha convertido en los últimos años en una actividad delictiva rentable, que se está desarrollando tanto a nivel nacional como internacional. Los grupos delictivos que se especializan en esta actividad se están desarrollando de manera dinámica y están atacando a una gama más amplia de víctimas. Teniendo en cuenta la participación activa de las víctimas y su implicación en escenarios delictivos y el efecto traumático que tiene en la mente de las víctimas, es preciso realizar una seria labor de prevención, teniendo en cuenta las especifidades a nivel local, nacional e internacional.»*

El fraude individual es un tipo de fraude en el que los delincuentes se dirigen a los ciudadanos comunes y corrientes. Persuaden a las víctimas para que cooperen y luego las estafan. Nuestra comprensión actual de este tipo de fraude está ligada principalmente a sus formas contemporáneas, con el phishing como el ejemplo más probable. No obstante, es importante reconocer que el fraude individual existe desde hace mucho tiempo. Las evoluciones tecnológicas de las últimas décadas sólo han permitido que estas estafas se industrialicen a mayor escala de lo que nunca se consideró posible. ¿Quién no ha recibido un e-mail de phishing alguna vez?

Como queda claro en la justificación de la Presidencia búlgara, las víctimas participan activamente en su victimización. El delincuente ha puesto sus ojos en el dinero de la víctima,

pero sólo puede acceder a él persuadiendo a la víctima de que lo haga. La táctica esencial para empujar a la víctima a esta relación complaciente se llama **ingeniería social**. Esta permite al delincuente obtener la confianza de la víctima que es crucial para el éxito de la estafa. La psicología social nos ofrece una mejor comprensión de este fenómeno. Apelando a los principios sociales cotidianos y explotando esta «debilidad humana», los delincuentes son capaces de activar lo que se llama la segunda vía de persuasión. La primera vía requiere una gran cantidad de pensamiento y esfuerzo cognitivo. La segunda, sin embargo, realmente no necesita ninguna elaboración; es una reacción casi inconsciente. Por ejemplo, al fingir ser una persona con autoridad, como un agente de policía, los delincuentes pueden obtener fácilmente un nivel de obediencia de sus víctimas. Estas reglas sociales y cognitivas tienen sus usos diarios, pero permiten a los delincuentes explotarlas para su propio beneficio.

Estas tácticas engañosas se utilizan en una amplia **variedad de estafas**. *419 estafas, estafas a ancianos, estafas románticas, fraudes del CEO, …* Las posibilidades son tan infinitas como la creatividad de los estafadores. Esta gama de estrategias engañosas permite a los estafadores dirigirse a la vez a un público muy amplio o adoptar un enfoque más específico. Cada vez más, este último parece ser el caso. Los estafadores se han dado cuenta de que si eligen cuidadosamente a sus víctimas, el «retorno de la inversión» es mayor. Los correos electrónicos de phishing son cada vez más sofisticados y están dirigidos a un objetivo o grupo concreto. El sorprendente último paso en esta evolución implica la combinación de tecnología nueva y antigua: el teléfono. El vishing, o phishing de voz, da la oportunidad de combinar las ventajas de Internet y del teléfono. Hacer una llamada telefónica a través de Internet tiene un coste muy bajo, es más difícil de rastrear y se puede automatizar. Además, usar el teléfono tiene otras ventajas: la gente se fía más y, debido al entorno más íntimo, el proceso de persuadir a las víctimas es más eficiente. Como ilustración del creciente nivel de sofisticación: los delincuentes incluso contratan a nativos para que las llamadas telefónicas parezcan lo más real posible.

Sin embargo, nuestra comprensión actual del fraude individual es limitada. A este delito se asocia una alta **cifra oscura** ya que en muchos casos no se denuncia. Las víctimas no saben que han sido víctimas, no lo perciben como suficientemente grave, no creen que la denuncia llevará a nada o simplemente no saben dónde denunciarlo. Además, debido al papel activo que desempeña la víctima en su propia victimización, los sentimientos de culpa y vergüenza impiden que las víctimas cuenten su historia. Algunas estafas incluso tienen mecanismos

incorporados que previenen la denuncia, ya que implican que las víctimas realicen acciones ilegales, con las que se autoincriminan. Denunciar la estafa sería como entregarse.

Esta cifra oscura también ha dado lugar al **mito** de que los ancianos son las principales víctimas de este delito, ya que son presa fácil. Algunos estudios han desmentido este mito, aunque debemos ser cautelosos debido a la limitada investigación disponible. No obstante, se informa de que la población más joven y el grupo de mediana edad son más susceptibles a las estafas. Otro mito que existe es que las víctimas suelen ser retratadas como personas incultas o analfabetos financieros, pero parece que ocurre lo contrario. Una posible explicación es la llamada «brecha entre conocimiento y acción», que implica que las personas son capaces de reconocer las señales de una estafa, pero no aplican este conocimiento a su propia situación.

Desgraciadamente, la existencia de «**listas de tontos**» no es un mito. Los estafadores telefónicos pueden contactar con sus víctimas al azar o mirando registros públicos, pero también comparten listas entre ellos con objetivos que ya han sido estafados. El uso de este tipo de listas es indicativo del alto nivel de victimización repetida. Por ejemplo, algunos estafadores intentarán «ayudar» a la víctima a recuperar sus bienes perdidos...

Como la represión de estos delitos es extremadamente difícil, la necesidad de prevención es alta. Sin embargo, se han realizado pocas investigaciones académicas y evaluativas sobre el fraude individual. No obstante, podemos plantear algunas conclusiones generales. La táctica de prevención más común es educar al público. Esto se puede hacer mediante una campaña de sensibilización general, pero sobre todo se pueden observar efectos positivos cuando se hace en el marco de algún tipo de formación. En esencia, el objetivo de esta formación es cerrar la «brecha entre conocimiento y acción» a la que nos hemos referido anteriormente. Otra táctica clave es trabajar con las víctimas. Debido a su papel activo y al riesgo existente de ser víctima en múltiples ocasiones, las víctimas deben recibir apoyo y ser conscientes de su posición específica.

Durante la Presidencia búlgara, la Secretaría recogió una serie de **buenas prácticas** sobre este tema. Estas pueden ser categorizadas según su grupo objetivo. Una primera categoría se centra en toda la población. Se trata de campañas de sensibilización, como los ejemplos de Bulgaria, Suecia, Bélgica o Europol. Consisten en anuncios de radio, carteles, folletos, aparatos etc. que proporcionan información útil al público y enseñan cómo protegerse. Una segunda serie de actividades está dirigida a los ancianos. Estas usan métodos más interactivos,

como es el caso en la República Checa. Los ancianos participan en una obra de teatro educativa interactiva donde aprenden sobre los métodos de engaño más comunes y cómo reaccionar ante ellos. Esta «experiencia vivida» debería permitirles reaccionar adecuadamente en escenarios de la vida real. La evaluación de este proyecto demostró que esta suposición era cierta, ya que el grupo rechazó las propuestas engañosas dos veces y media más que un grupo de control que no vio la obra. La última categoría de actividades de prevención se centra en las víctimas. Los ejemplos de Australia, Reino Unido y Canadá demostraron la necesidad de este tipo de prevención. Sin embargo, incluso a nivel mundial, existen pocos servicios de apoyo a las víctimas de fraudes individuales.

Finalmente, la Secretaría de la REPD organizó un taller con diferentes expertos para elaborar algunas **recomendaciones** sobre cómo prevenir las estafas telefónicas. Estas se estructuran de acuerdo con las cinco estrategias de prevención del delito situacional. La primera estrategia posible es aumentar el esfuerzo que un delincuente tiene que hacer para que la estafa tenga éxito. Restringiendo la publicación y el acceso a los números de teléfono ya se puede lograr esto. Otra técnica podría consistir en limitar la cantidad de números de teléfono que se permite tener a una persona o, al menos, vincularlos a una cuenta bancaria o a un número de identificación.

Una segunda estrategia consiste en aumentar los riesgos. En este contexto, es esencial compartir información. Esto no debe detenerse en las fronteras del sector público o privado, ni en las fronteras nacionales. Todos los socios tienen una pieza de información importante para resolver el puzzle. Saber a qué te enfrentas aumenta las posibilidades de evitar que suceda en primer lugar. Huelga decir que presentar una denuncia debería ser más sencillo y accesible. Es necesario recoger información antes de poder compartirla. Se hicieron otras recomendaciones para reducir el anonimato de la persona que llama, haciendo casi imposible falsificar su ubicación. El software de reconocimiento de voz también podría ser de interés aquí.

La reducción de las recompensas que se pueden obtener cometiendo este delito es una tercera estrategia para evitar los fraudes telefónicos. La principal recomendación en este sentido es la incautación de los bienes obtenidos ilegalmente. Para ello, la vigilancia del flujo de dinero es crucial para detectar transacciones sospechosas. Nuestros expertos recomendaron una iniciativa de toda la Unión Europea con el sector bancario para facilitar este proceso.

Otra estrategia es reducir las provocaciones. En este contexto es importante no compartir demasiada información sobre la forma exacta en que se ejecutó la estafa, ya que así se evitará que se produzcan imitaciones. Además, podría ayudar a prevenir algunas formas de victimización repetida. La última estrategia es eliminar las excusas. Esta se centra principalmente en la sensibilización sobre las estafas telefónicas y cómo protegerse. Las buenas prácticas anteriormente mencionadas se presentan aquí como ejemplos clave. Las campañas de sensibilización deberían difundir el mismo mensaje. Por lo tanto, es necesario establecer una cooperación entre los sectores público y privado y a nivel internacional que sea lo más coherente posible: *simplemente di no.*