1
00:01:43.150 --> 00:01:45.939
Efraín Botello-Cisneros: Hola, buenos días a todos.

2
00:01:47.400 --> 00:02:05.800
Efraín Botello-Cisneros: Hola, buenos días. Bienvenidos al cuarto y último webinar de Desmitificando el DOJ de la serie de 2025. Mi nombre es Efraín Botellos Cisneros y soy el gerente de difusión comunitaria para la región de Gran Sacramento y Valle Central de la Oficina de Conciencia, Respuesta y Participación Comunitaria.

3
00:02:05.800 --> 00:02:12.269
Efraín Botello-Cisneros: También conocida como CARE, aquí en el Departamento de Justicia de California. Tengo el privilegio de ser su presentador hoy.

4
00:02:12.300 --> 00:02:20.589
Efraín Botello-Cisneros: Y mi colega, Ben Nate, estará publicando información importante en el chat, así que también presten atención ahí durante la presentación.

5
00:02:21.360 --> 00:02:29.779
Efraín Botello-Cisneros: Tengan en cuenta que hay subtítulos ocultos disponibles. Para acceder a ellos, seleccionen la pestaña More (Más) en la barra del menú en la parte inferior de su pantalla.

6
00:02:29.910 --> 00:02:33.650
Efraín Botello-Cisneros: Deberían ver un icono que se ve como el de la imagen de aquí.

7
00:02:33.760 --> 00:02:36.730
Efraín Botello-Cisneros: Una vez que hagan clic en él, los subtítulos deberían aparecer.

8
00:02:36.860 --> 00:02:49.959
Efraín Botello-Cisneros: Se traducirá al español esta presentación y se publicará en nuestro sitio web en las próximas semanas. Para ajustar la vista, pueden mover el deslizador vertical en su pantalla para ampliar o minimizar la presentación.

9
00:02:54.610 --> 00:03:12.710
Efraín Botello-Cisneros: El tema central de la presentación de Desmitificando el DOJ de hoy es la Sección de Delitos Cibernéticos del Departamento de Justicia de California. Hoy tenemos un gran programa para ustedes, comenzando con comentarios del asistente especial del fiscal general, Jamal Anderson, quien trabaja como el asesor principal en

política para el fiscal general en asuntos de justicia penal y cumplimiento de la ley.

10
00:03:12.710 --> 00:03:24.219
Efraín Botello-Cisneros: Después, tenemos el honor de escuchar a expertos de la Sección de Delitos Cibernéticos, incluyendo a la asistente legal sénior, Sam Terry y al auditor investigador supervisor, Lawrence Wold.

11
00:03:24.220 --> 00:03:28.149
Efraín Botello-Cisneros: Así como al fiscal general adjunto supervisor, Dorian Peters.

12
00:03:28.170 --> 00:03:34.890
Efraín Botello-Cisneros: Estarán compartiendo más sobre el trabajo de la Sección de Delitos Cibernéticos y hablarán sobre asuntos de la evolución de delitos relacionados con la tecnología.

13
00:03:35.580 --> 00:03:46.739
Efraín Botello-Cisneros: Después de su presentación, responderemos algunas de sus preguntas. Gracias a todos los que enviaron preguntas con antelación. Las hemos compartido con los presentadores, así que harán todo lo posible por responderlas en su presentación.

14
00:03:46.870 --> 00:03:52.850
Efraín Botello-Cisneros: Si tienen preguntas durante la presentación, todavía pueden enviarlas mediante la caja de preguntas y respuestas en la parte inferior de su pantalla.

15
00:03:52.990 --> 00:04:03.600
Efraín Botello-Cisneros: Tengan en cuenta que es posible que no podamos responder ninguna pregunta relacionada con investigaciones activas u otros temas sensibles para proteger la integridad de nuestro trabajo. Gracias por su comprensión.

16
00:04:05.760 --> 00:04:15.309
Efraín Botello-Cisneros: Si hoy nos acompaña como reportero o está colaborando con la prensa, envíe sus preguntas a agpressoffice@doj.ca.gov.

17
00:04:15.500 --> 00:04:32.980
Efraín Botello-Cisneros: Y por último, les agradeceríamos si pudieran tomarse unos minutos para completar una breve encuesta después del programa de hoy, ya que sus comentarios nos ayudarán a mejorar para próximos eventos. Sin más preámbulo, es un placer presentar al asistente especial del fiscal general, Jamal Anderson.

18
00:04:32.980 --> 00:04:35.540
Efraín Botello-Cisneros: Sr. Anderson, puede comenzar.

19
00:04:36.190 --> 00:04:38.599
Jamal Anderson: Gracias Efraín y buenos días.

20
00:04:38.920 --> 00:04:45.909
Jamal Anderson: Mi nombre es Jamal Anderson y soy el asistente especial del fiscal general del Departamento de Justicia de California.

21
00:04:46.030 --> 00:05:04.919
Jamal Anderson: En ese sentido, trabajo como el asesor legal y político del fiscal general sobre seguridad pública, justicia penal, cumplimiento de la ley y armas de fuego. Me emociona darles la bienvenida a nuestro webinar esta mañana en nombre del fiscal general y de todos los empleados del Departamento de Justicia de California.

22
00:05:04.960 --> 00:05:15.280
Jamal Anderson: Espero que tomen esta oportunidad para aprender un poco más acerca del increíble trabajo de nuestra Sección de Delitos Cibernéticos que dirige nuestra asistente sénior del fiscal general, Jeanette Jerome.

23
00:05:15.660 --> 00:05:28.319
Jamal Anderson: Sería complicado leer las noticias actualmente, ya sea en un periódico, para quienes todavía lo hacen, o en línea, y no encontrar un problema relacionado con el trabajo de nuestra Sección de Delitos Cibernéticos.

24
00:05:28.470 --> 00:05:45.980
Jamal Anderson: Desde delitos por Internet contra nuestros residentes más vulnerables, incluyendo adultos mayores y niños, hasta robo de identidad y estafas con criptomonedas, nuestra Sección de Delitos Cibernéticos encabeza el camino en el trabajo, frecuentemente desapercibido, pero siempre eficaz, para mantener seguros a todos los californianos.

25
00:05:46.220 --> 00:06:01.090
Jamal Anderson: A menudo, al fiscal general le gusta decir que en el Departamento de Justicia de California la seguridad pública es la prioridad número 1, 2 y 3. Y nuestra extraordinaria Sección de Delitos Cibernéticos se adhiere a ese mantra todos los días.

26
00:06:01.260 --> 00:06:17.970
Jamal Anderson: El trabajo que hacen es extraordinario y de vital importancia, y me emociona que hoy tendrán la oportunidad de conocer más

sobre ese trabajo. Espero que el webinar de hoy les resulte útil y esclarecedor y, nuevamente, bienvenidos y gracias por acompañarnos.

27
00:06:20.960 --> 00:06:24.469
Jamal Anderson: Con eso, le doy la palabra a la asistente legal sénior

28
00:06:24.620 --> 00:06:27.150
Jamal Anderson: o más bien, analista, Sam Terry.

29
00:06:28.350 --> 00:06:44.660
Victoria Terry: ¡Buenos días! Les doy la bienvenida a todos. Mi nombre es Sam Terry. Soy analista legal sénior de la Sección de Delitos Cibernéticos. Antes nos llamábamos Unidad de Delitos Electrónicos. Comencé a trabajar en el Departamento de Justicia en enero de 2007. Comencé en la Sección Legal del Gobierno y,

30
00:06:44.980 --> 00:07:01.109
Victoria Terry: Fue aproximadamente en 2008 cuando me transfirieron a la Unidad de Reclamos Falsos y Delitos Especiales, y es ahí donde tuve mi primera introducción a la unidad de procesamiento del Departamento de Justicia.

31
00:07:01.110 --> 00:07:21.440
Victoria Terry: Quería señalar algo que considero muy importante para mí y es que utilicé el Programa de Movilidad Ascendente mientras estuve ahí. Ya tenía completados mis estudios paralegales, pero quería avanzar en mi carrera, entonces usé ese programa para regresar a la escuela y obtener mi título en administración de justicia.

32
00:07:21.440 --> 00:07:39.260
Victoria Terry: Si alguien está pensando en hacerlo, le recomendaría mucho investigar sobre eso para obtener ayuda para su carrera. Es un poco sobre mí. También, a inicios de mis 20 fui bombera durante 6 años para CDF y lo disfruté muchísimo.

33
00:07:39.280 --> 00:07:48.410
Victoria Terry: Para mis 40 años, buceé en el Gran Agujero Azul y fue mi primera vez buceando en Belice. Eso también fue extraordinario, y también me encanta el género de crímenes reales.

34
00:07:48.410 --> 00:08:04.880
Victoria Terry: En cada incidente de mi vida pienso en alguna escena de dateline; eso no es muy bueno. De lo que quiero hablar primero es de

35
00:08:05.310 --> 00:08:17.350

Victoria Terry: la línea de tiempo de nuestra sección. Voy a darles un poco de historia, porque es donde vienen nuestros fondos, es de donde viene una parte de los fondos para nuestra sección.

36
00:08:17.350 --> 00:08:31.199
Victoria Terry: En 1998, el senado aprobó el Proyecto de Ley SB 1734 y el AB821. Este fue el Programa de Detención y Procesamiento de Robos de Alta Tecnología,

37
00:08:31.290 --> 00:08:45.150
Victoria Terry: junto con el AB821 que fue el Comité Asesor contra Delitos de Alta Tecnología. Esto se creó para combatir e investigar el procesamiento de delitos de alta tecnología

38
00:08:45.150 --> 00:09:02.270
Victoria Terry: incluyendo robo de identidad, de hecho originalmente no era robo de identidad, era lavado de dinero y delitos de cuello banco, robo de valores y todo eso. En 2001, el programa se amplió para incluir robo de identidad.

39
00:09:02.300 --> 00:09:11.540
Victoria Terry: Algo realmente significativo es que aproximadamente en el período de 2008 es cuando CDAA y la oficina del AG agregaron

40
00:09:11.540 --> 00:09:25.719
Victoria Terry: DAG y ADA al programa. Estaban integrados en estos grupos de trabajo para ayudar a procesar los casos que les llevaban y también para liberar la carga de agencias más pequeñas

41
00:09:25.720 --> 00:09:28.999
Victoria Terry: que estaban teniendo problemas para combatir estos delitos.

42
00:09:29.000 --> 00:09:35.869
Victoria Terry: Alrededor de 2009, ya se estaba escuchando hablar de las criptomonedas.

43
00:09:35.870 --> 00:09:54.740
Victoria Terry: En enero fue Bitcoin. Bitcoin, Bitcoin, Bitcoin. Todo era sobre Bitcoin. Era una moneda nueva, y en ese momento nuestra unidad estaba tratando de comprender qué era eso. Alrededor de 2010, empezaron los reportes desenfrenados de robo de identidad.

44
00:09:54.740 --> 00:10:03.450

Victoria Terry: Ese era uno de los problemas principales que estábamos teniendo en nuestra unidad, el robo de identidad.

45
00:10:03.450 --> 00:10:15.130
Victoria Terry: Creo que fue alrededor de ese momento cuando la AG Harris anunció que iba a crear la Unidad de Delitos Electrónicos dándose cuenta de que

46
00:10:15.130 --> 00:10:31.470
Victoria Terry: los delincuentes estaban usando teléfonos inteligentes y dispositivos digitales para victimizar a las personas en línea y en la vida real. Ahora volviendo a esto, quiero explicar los grupos de trabajo. Sobre los grupos de trabajo en sí, hay 5 en 5 regiones diferentes.

47
00:10:31.470 --> 00:10:51.059
Victoria Terry: Primero está el de San Diego. Se llama Equipo de Respuesta de Alta Tecnología para Delitos Informáticos y Tecnológicos. Abreviado CATCH. Cubre los condados de Imperial, San Diego y Riverside. Si nos movemos a Los Ángeles, tenemos el

48
00:10:51.060 --> 00:11:08.110
Victoria Terry: Grupo de Trabajo de Alta Tecnología del Sur de California. Cubre el área de LA y los condados de Orange y Ventura. Si nos movemos a Silicon Valley, tenemos al Equipo Informático Aliado de Cumplimiento Rápido. Abreviado REACT.

49
00:11:08.110 --> 00:11:12.559
Victoria Terry: Cubre San José, el condado de Alameda, San Francisco,

50
00:11:12.560 --> 00:11:27.240
Victoria Terry: los condados de San Mateo, Santa Cruz y Santa Clara. Hay otro si nos movemos al condado de Marin en Napa que es el Grupo de Trabajo para Delitos Informáticos del Norte de California, abreviado NC3TF.

51
00:11:27.240 --> 00:11:42.450
Victoria Terry: Cubre 13 condados, del condado de Contra Costa al de Shasta. Y el último está en el Valle en Sacramento. Se llama Grupo de Trabajo de Delitos Altos del Valle de Sacramento.

52
00:11:42.480 --> 00:11:51.340
Victoria Terry: Representa o cubre alrededor de 17 condados, desde El Dorado hasta el área de Stanislaus.

53
00:11:51.340 --> 00:12:05.849

Victoria Terry: Cuando nos crearon, delitos especiales ya estaba trabajando con ese tipo de delitos, los tipos de delitos que Delitos Electrónicos eventualmente comenzó a cubrir. Había DAG que ya estaban integrados en estos grupos de trabajo,

54
00:12:05.850 --> 00:12:08.959
Victoria Terry: tres para ser específicos. Cuando nos crearon,

55
00:12:08.980 --> 00:12:21.569
Victoria Terry: les preguntaron si querían comenzar a cubrir específicamente los delitos electrónicos y, como ya eran expertos en el área, simplemente transicionaron a la Unidad de Delitos Electrónicos. Empezamos con 3 DAG,

56
00:12:21.570 --> 00:12:42.619
Victoria Terry: un analista legal senior y un auditor. Éramos muy pequeños. Durante aproximadamente 10 años, antes de que cambiáramos a ser la Sección de Delitos Cibernéticos, solo trabajábamos con aproximadamente 10 personas, 5 DAG y teníamos muchos casos en los que trabajábamos.

57
00:12:42.620 --> 00:12:48.020
Victoria Terry: En esta siguiente diapositiva quiero mostrarles

58
00:12:48.210 --> 00:13:12.109
Victoria Terry: la diferencia entre delitos y el motivo por el que realmente nos crearon, por qué fue necesario que la AG Harris creara la unidad. Aquí pueden ver el promedio de delitos monetarios y de delitos domésticos, que de cierto modo se equilibraron. Realmente no estaban cambiando demasiado, y cuando observamos los delitos informáticos, podemos ver que alrededor de 2009 estos simplemente

59
00:13:12.110 --> 00:13:14.765
Victoria Terry: se dispararon.

60
00:13:15.160 --> 00:13:21.350
Victoria Terry: Creo que esa fue la importancia de crear la unidad. Entonces,

61
00:13:21.930 --> 00:13:27.870
Victoria Terry: a lo largo de los años hemos procesado muchos delitos diferentes, desde robo de identidad,

62
00:13:27.870 --> 00:13:48.479
Victoria Terry: piratería, lavado de dinero, falsificación de bienes, acoso cibernético y robo con allanamiento de morada. Al inicio,

básicamente la premisa era que si el delito se estaba cometiendo por Internet, era un delito de Internet; un delito electrónico. Entonces, estábamos procesando muchos de estos delitos, creo que el más importante fue el de robo de identidad.

63
00:13:48.480 --> 00:13:55.860
Victoria Terry: El robo de identidad ocurre cada 22 segundos en Estados Unidos.

64
00:13:55.910 --> 00:14:02.169
Victoria Terry: Quiero hacer un resumen,

65
00:14:02.490 --> 00:14:11.309
Victoria Terry: disculpen, la dispositiva no cambia, un resumen de los delitos por Internet que ocurrieron en 2010. Son los que se reportaron al FBI.

66
00:14:11.310 --> 00:14:25.199
Victoria Terry: Se llama IC3, Centro de Quejas de Delitos Cibernéticos, abreviado IC3. Es a donde acuden si son víctimas de un delito por Internet. Pueden visitar el sitio web del FBI y reportar delitos que les ocurran.

67
00:14:25.310 --> 00:14:30.869
Victoria Terry: Alrededor de 2010, recibimos aproximadamente unos 300,000 casos reportados.

68
00:14:30.870 --> 00:14:45.870
Victoria Terry: Las criptomonedas ni siquiera existían en ese momento en el FBI, por lo que no llevaban el seguimiento de eso. No había delitos con criptomonedas o algo por el estilo hasta el momento. Estábamos trabajando con muchos robos de identidad.

69
00:14:45.870 --> 00:14:57.440
Victoria Terry: El siguiente año del que hablaré es 2024 porque quería señalar que las denuncias que recibimos, como pueden ver, fueron 859,000. Es algo

70
00:14:57.520 --> 00:15:11.129
Victoria Terry: enorme. La pérdida financiera ronda los mil millones. Y creo que es en 2024 cuando comenzaron a llevar el seguimiento de las criptomonedas, quizás 2022 o 2023.

71
00:15:11.320 --> 00:15:30.629

Victoria Terry: Pero en 2024 se reportó que hubo una pérdida de más de $9 mil millones en criptomonedas. Lo siguiente que les estoy mostrando ahora es el período de 2012 a 2024, cuando nuestra unidad ya existía, y muestra los diferentes delitos reportados al FBI.

72
00:15:30.710 --> 00:15:46.550
Victoria Terry: Pueden ver que alrededor de 2017 es cuando comienza a dispararse de manera significativa cada año tanto el número de denuncias como la pérdida reportada.

73
00:15:46.550 --> 00:15:58.340
Victoria Terry: Aquí empiezo en el 2017 porque es cuando realmente empezamos a recibir reportes sobre criptomonedas. No había muchas pérdidas. Las personas decían: "Me estafaron con esta

74
00:15:59.030 --> 00:16:18.069
Victoria Terry: moneda en línea que no sé qué es" y empezaban a reportarlo, pero realmente no estaban perdiendo valor y no se empieza a notar hasta alrededor de 2021, 2022 y especialmente 2023 porque ahí es cuando llegaron los reportes al FBI sobre denuncias de criptomonedas. Así que,

75
00:16:18.910 --> 00:16:19.970
Victoria Terry: nuestra

76
00:16:20.580 --> 00:16:27.739
Victoria Terry: unidad ha cambiado significativamente a lo largo de los años. Como dije, al inicio trabajábamos mucho con robo de identidad.

77
00:16:27.740 --> 00:16:47.510
Victoria Terry: Y los protocolos de seguridad desde ese entonces se han establecido y ese tipo de delito ha disminuido. Como dije antes, en realidad cualquier delito se puede relacionar con el Internet, en ese momento en nuestra sección o unidad, queríamos asegurarnos de que estuviéramos representando y

78
00:16:47.510 --> 00:16:57.869
Victoria Terry: considerando los delitos que ocurrían. Las criptomonedas son algo con lo que comenzamos de manera frontal y francamente

79
00:16:58.010 --> 00:17:00.589
Victoria Terry: creo que las criptomonedas no son buenas.

80
00:17:00.740 --> 00:17:18.319

Victoria Terry: No creo que tengan motivos legítimos para existir, entonces elegí no especializarme en criptomonedas simplemente porque no creo en ellas. Este es el panorama de las criptomonedas.

81
00:17:18.930 --> 00:17:32.020
Victoria Terry: Pueden ver los reportes, realmente no hay mucho. La brecha de valor está a nivel de las criptomonedas, pero los reportes comienzan a llegar. Como pueden ver en 2014 hay una gran

82
00:17:32.490 --> 00:17:50.840
Victoria Terry: brecha. ¿Es de 300, 500, 663 millones? En 2014 ocurrió el hackeo de Mt. Gox en el que se robaron aproximadamente 850,000 Bitcoin.

83
00:17:50.840 --> 00:17:59.080
Victoria Terry: El valor de las Bitcoin obviamente cambia, pero su valor en ese momento era de $450 millones. Ha habido algo de

84
00:17:59.400 --> 00:18:12.260
Victoria Terry: información que ha salido desde entonces, pero creo que pudieron recuperar aproximadamente 200,000 Bitcoin de ese incidente. Entonces,

85
00:18:12.260 --> 00:18:21.339
Victoria Terry: como pueden ver las tendencias de robo aumentan con las criptomonedas. Es un

86
00:18:21.590 --> 00:18:38.039
Victoria Terry: delito que será muy difícil de procesar, pero les puedo decir que nuestra Sección está tratando de enfrentarlo a toda velocidad. Lo bueno es que tengo un colega al que le encanta hablar de criptomonedas.

87
00:18:38.040 --> 00:18:42.130
Victoria Terry: Le voy a dar la palabra a Lawrence

88
00:18:42.130 --> 00:18:46.940
Victoria Terry: y él les puede hablar mucho más de las criptomonedas. Gracias por escuchar.

89
00:18:50.920 --> 00:19:01.189
Lawrence Wold: Gracias, Sam. Soy Lawrence Wold. Soy CPA de profesión. Tengo un MBA en finanzas y me le tengo un entusiasmo especial.

90
00:19:01.310 --> 00:19:15.300

Lawrence Wold: Me uní a la Sección de Delitos Cibernéticos hace casi 3 años. Antes de eso, trabajaba en el área de fraudes en la atención médica y también en el área de fraudes corporativos, y esta era un área que tenía una necesidad.

91
00:19:15.450 --> 00:19:27.869
Lawrence Wold: Me encantan las redes. Las redes son muy valiosas para que las personas traten de compartir información. Pueden encontrarme en LinkedIn. Debo decir que las opiniones expresadas

92
00:19:27.870 --> 00:19:39.039
Lawrence Wold: son solo mías y si quieren enviarme cumplidos, comentarios o críticas, pueden comunicarse conmigo en lawrence.wold@doj.

93
00:19:39.100 --> 00:19:40.570
Lawrence Wold: Ca.gov.

94
00:19:41.550 --> 00:19:55.180
Lawrence Wold: Estos son algunos datos sobre las criptomonedas. No soy defensor de las criptomonedas o de que las personas normales las compren, pero son mucho más que una moda pasajera.

95
00:19:55.260 --> 00:20:02.899
Lawrence Wold: Se van a quedar, puede que crezcan, que cambien, que se modifiquen, pero no van a desaparecer.

96
00:20:03.200 --> 00:20:20.160
Lawrence Wold: Uno de los datos más básicos es que se basan en computadoras. Es posible que hayan visto imágenes de un token de Bitcoin. Esos son solo ejemplos, un ejemplo visual, pero no es real.

97
00:20:20.350 --> 00:20:32.970
Lawrence Wold: Es casi imposible regular las criptomonedas. Cruzan fronteras, se mueven fuera del sistema bancario y fuera de la regulación gubernamental, en su gran mayoría.

98
00:20:33.320 --> 00:20:45.210
Lawrence Wold: Y otro de los datos básicos es que todos han escuchado de Bitcoin y las criptomonedas, pero muy pocos saben realmente cómo funcionan y profundizan en ello.

99
00:20:45.470 --> 00:20:57.169
Lawrence Wold: Como dije, es muy fácil transferirlas alrededor del mundo, lo que les da algo de utilidad, pero también las hace casi ideales para uso de los delincuentes.

100
00:20:58.490 --> 00:21:16.710
Lawrence Wold: Yo hago una analogía entre el entorno de las criptomonedas y el viejo oeste. Está lleno de emoción, pero también de estafadores. Hay promesas, a menudo falsas, de ganancias enormes.

101
00:21:17.070 --> 00:21:30.179
Lawrence Wold: Especialmente, ahora que Bitcoin se está anunciando en el área de negocios. Siempre se mueve y recientemente ha crecido cerca de $100,000 por moneda.

102
00:21:30.790 --> 00:21:35.739
Lawrence Wold: Lo escalofriante para nosotros es que crea

103
00:21:35.880 --> 00:21:53.400
Lawrence Wold: algo que llamamos miedo a perderse de algo o FOMO. Con toda esa emoción, las personas piensan "Hey, yo también quiero hacerlo" sin comprender totalmente qué es o cuáles son los riesgos, y esto crea la enorme posibilidad de que haya fraudes, estafas y robos.

104
00:21:54.500 --> 00:21:58.810
Lawrence Wold: Hay muchos tipos diferentes de estafas que usan criptomonedas.

105
00:21:58.950 --> 00:22:11.269
Lawrence Wold: Casi cualquier persona que tenga un celular ha recibido un mensaje de texto aleatorio. Podría decir "Hola, doctor, necesito llevar a Fluffy para su siguiente cita".

106
00:22:11.620 --> 00:22:20.430
Lawrence Wold: Estos se generan mediante IA o bancos de personas que los envían aleatoriamente.

107
00:22:20.430 --> 00:22:32.320
Lawrence Wold: Esperan encontrar buenas personas que sean educadas, luego tratan de construir una relación y luego les sugieren que comiencen a invertir en criptomonedas.

108
00:22:33.080 --> 00:22:42.929
Lawrence Wold: Muchas veces, si usan LinkedIn, reciben mensajes aleatorios por LinkedIn para empleos o de alguien que simplemente quiere ser su amigo.

109
00:22:43.150 --> 00:22:47.289

Lawrence Wold: Hay estafas al servicio de jurado y también fiscales.

110
00:22:47.290 --> 00:23:04.520
Lawrence Wold: Son en las que reciben llamadas telefónicas de alguien que suena muy real. Dicen "Faltó a su deber de jurado o debe impuestos. Vamos a obtener una orden de arresto. La única manera de que no lo arrestemos es si va inmediatamente a su banco,

111
00:23:04.600 --> 00:23:08.199
Lawrence Wold: retira un montón de efectivo y lo envía mediante un ATM para Bitcoin".

112
00:23:09.120 --> 00:23:24.590
Lawrence Wold: Estafas de extorsión sexual. Estas son horribles, acechan a adolescentes y tratan de construir una amistad, crean una personalidad falsa y luego comienzan a querer intercambiar fotos, y después de que el adolescente

113
00:23:24.590 --> 00:23:37.469
Lawrence Wold: envía la foto, tratan de chantajearlo diciendo "A menos que nos envíes dinero mediante un ATM para Bitcoin, vamos a enviar estas imágenes a todos tus amigos".

114
00:23:37.710 --> 00:23:53.010
Lawrence Wold: Como mencioné, estafas de empleo. A menudo, a las personas que están desesperadas por un empleo, las contactan, o ellas solicitan un empleo en un sitio web y les dicen "Para su revisión de antecedentes, debe enviar algunas Bitcoin".

115
00:23:53.880 --> 00:24:03.800
Lawrence Wold: También están las estafas por mensajería. Yo recibo estafas de peaje aproximadamente 2-3 veces al mes.

116
00:24:03.980 --> 00:24:08.710
Lawrence Wold: Y una de las cosas tristes es que las estafas de peaje son falsas.

117
00:24:08.880 --> 00:24:15.979
Lawrence Wold: Pero solo cuestan alrededor de $25, $30, por lo que muchas personas están dispuestas a pagarlas sin saber que no son reales.

118
00:24:16.520 --> 00:24:27.140
Lawrence Wold: Una de las peores y más grandes cosas con la que nos enfrentamos son las estafas de romance. Son cuando las personas usan sitios web de citas reales

119
00:24:27.300 --> 00:24:40.140
Lawrence Wold: y comienzan a desarrollar una amistad, simpatía, y de repente, encuentran a la persona de sus sueños. Pues la persona de sus sueños está fuera del estado o en una parte diferente del estado.

120
00:24:40.140 --> 00:24:55.899
Lawrence Wold: Construyen una relación muy intensa y de confianza, y luego el estafador trata de que la persona dé o comparta dinero para invertirlo en criptomonedas.

121
00:24:57.100 --> 00:25:05.860
Lawrence Wold: Los ATM para criptomonedas prácticamente no tienen un objetivo legítimo, en mi opinión.

122
00:25:05.950 --> 00:25:18.610
Lawrence Wold: Por eso pueden encontrarlos en gasolineras o licorerías. No los encuentran en los bancos. Nuestra oficina está trabajando y evaluando legislaciones que tratarán de regular

123
00:25:18.610 --> 00:25:36.639
Lawrence Wold: los ATM para Bitcoin, tratarán de limitar la cantidad que una persona puede depositar y también tratará de obligar a que las compañías de las máquinas de ATM tengan mejores regulaciones y advertencias.

124
00:25:38.290 --> 00:25:53.949
Lawrence Wold: Para analizar cómo funciona una estafa típica uso el video de John Oliver. Tenía un gran segmento que está publicado. A algunas personas les gusta su humor, a otras no, pero tenía un gran segmento sobre a estafa de pig butchering.

125
00:25:54.270 --> 00:26:00.209
Lawrence Wold: Como mencioné antes, tratan de que su objetivo sean personas buenas, de confianza.

126
00:26:00.340 --> 00:26:14.109
Lawrence Wold: O personas que quieren obtener ganancias rápidas que no entienden muy bien cómo funcionan los mercados financieros y piensan "Claro, puedo triplicar mi dinero en un mes".

127
00:26:14.730 --> 00:26:26.299
Lawrence Wold: A menudo hay un componente romántico en estas estafas de inversión. A veces, principalmente es una estafa de romance, pero a veces hay un componente romántico.

128
00:26:27.210 --> 00:26:40.049
Lawrence Wold: El propósito principal es construir confianza. Les piden que metan dinero en un sitio web. Con frecuencia son sitios web falsos, hablaré de eso en un minuto.

129
00:26:40.150 --> 00:26:45.540
Lawrence Wold: Y estos sitios web muestran que está obteniendo muchas ganancias.

130
00:26:46.360 --> 00:26:48.790
Lawrence Wold: Esto provoca que las víctimas

131
00:26:48.920 --> 00:26:57.009
Lawrence Wold: inviertan más y más. Estas ganancias crean un pico de dopamina y piensan que van a poder ganar muchísimo dinero.

132
00:26:57.340 --> 00:27:10.520
Lawrence Wold: Las personas comienzan a invertir todo lo que pueden, refinancian su casa, piden dinero prestado a amigos y familiares, vacían su cuenta para la jubilación.

133
00:27:10.940 --> 00:27:13.139
Lawrence Wold: Pero piensan que están ganando 10 veces más.

134
00:27:13.430 --> 00:27:27.139
Lawrence Wold: En promedio, las víctimas de estafas, y estos son nuestros datos sobre delitos cibernéticos cerca del promedio nacional, es de aproximadamente $132,000.

135
00:27:27.660 --> 00:27:32.000
Lawrence Wold: He tenido víctimas como un abogado jubilado que

136
00:27:32.120 --> 00:27:38.220
Lawrence Wold: perdió un millón de dólares. He tenido estudiantes universitarios que perdieron $2,000 o $6,000.

137
00:27:38.390 --> 00:27:40.289
Lawrence Wold: Es un gran

138
00:27:40.410 --> 00:27:45.630
Lawrence Wold: golpe para ellos y de hecho, es una parte enorme de sus ahorros de toda la vida.

139
00:27:46.490 --> 00:27:51.540
Lawrence Wold: En una estafa típica, cuando las personas quieren cobrar

140
00:27:51.740 --> 00:28:08.950
Lawrence Wold: los estafadores les dicen que hay una tarifa oculta, una comisión o una retención de impuestos y eso hace que pidan más dinero prestado o que tomen dinero que ni siquiera querían enviar. Pero piensan que obtendrán a cambio $800,000.

141
00:28:09.720 --> 00:28:24.850
Lawrence Wold: Se llama pig butchering porque cuando se destaza a un cerdo, los carniceros tratan de aprovechar de la cola al hocico, y todo lo que está en medio. Estos estafadores no son diferentes. Tratan de tomar cada centavo que pueden.

142
00:28:27.460 --> 00:28:28.420
Lawrence Wold: Entonces,

143
00:28:28.710 --> 00:28:45.160
Lawrence Wold: hablando de los sitios web de inversión fraudulentos, a primera vista muchos se ven bastante bien. Muchos tienen buenos gráficos, gráficos que se mueven y algunos tienen lenguaje generado de IA.

144
00:28:45.380 --> 00:28:51.420
Lawrence Wold: Toman prestado o roban enlaces hacia sitios web reales.

145
00:28:51.600 --> 00:29:00.220
Lawrence Wold: Muchos tienen nombres que tratan de hacerlos creíbles. Por ejemplo, CoinbaseInvest.com.

146
00:29:01.230 --> 00:29:06.209
Lawrence Wold: Desafortunadamente, estos sitios web son muy fáciles de crear.

147
00:29:06.500 --> 00:29:16.620
Lawrence Wold: La mayoría de los que encontramos tienen sedes en países del tercer mundo. Vietnam, Camboya, Myanmar y países que eran del bloque del este.

148
00:29:17.470 --> 00:29:34.010
Lawrence Wold: Desafortunadamente, muchas de las personas que los generan o muchos de los trabajadores son en realidad víctimas de trata de

personas. Son las personas que envían los mensajes de texto aleatorios, que llaman y que están en las funciones de chat.

149
00:29:35.310 --> 00:29:49.490
Lawrence Wold: Se han hecho algunos esfuerzos y avances para cerrar estos centros de estafas. Desafortunadamente, son enormemente rentables para gobiernos corruptos, por lo que no se están deteniendo tanto como nos gustaría.

150
00:29:50.840 --> 00:29:51.710
Lawrence Wold: Entonces,

151
00:29:52.330 --> 00:30:03.940
Lawrence Wold: ¿qué hacemos en Delitos Cibernéticos del DOJ? Investigamos pistas y denuncias, y a menudo usamos un software muy sofisticado,

152
00:30:03.940 --> 00:30:15.860
Lawrence Wold: TRM Labs, así como análisis en cadena, de hecho hacemos análisis de blockchain y tratamos de rastrear y congelar fondos si van hacia un sitio web real.

153
00:30:16.070 --> 00:30:31.440
Lawrence Wold: Desafortunadamente, no es tan exitoso como nos gustaría. Muchos estafadores saben que si usan una plataforma de intercambio de China o en el extranjero y cobran,

154
00:30:31.450 --> 00:30:41.970
Lawrence Wold: esas plataformas no necesitan la información o el KYC del cliente. No son muy cooperativos con la policía de EE. UU.

155
00:30:42.840 --> 00:30:51.780
Lawrence Wold: Desafortunadamente, lo que se recupera es poco y no sucede muy seguido. Cuando recuperamos algo, nos emociona y alegra hacerlo.

156
00:30:51.920 --> 00:30:58.409
Lawrence Wold: Pero, definitivamente entrevistamos a las víctimas. En mi

157
00:30:58.840 --> 00:31:16.589
Lawrence Wold: experiencia, las víctimas frecuentemente se sienten avergonzadas. Desafortunadamente, no quieren contarle a su familia y amigos que fueron víctimas. Están emocionalmente consternadas. Especialmente con las estafas de romance, se sienten traicionadas. Se

158
00:31:16.610 --> 00:31:29.550

Lawrence Wold: dedican emocionalmente a una persona y luego se enteran de que esa persona era falsa y les robó muchos de sus ahorros de toda la vida.

159
00:31:30.100 --> 00:31:35.060
Lawrence Wold: Algo en lo que hemos tenido éxito es en cerrar sitios web falsos.

160
00:31:35.180 --> 00:31:51.460
Lawrence Wold: Y podemos obtener la información por las entrevistas con las víctimas, el rastreo y tenemos acceso a bases de datos nacionales de la policía. Entonces, si veo que aparece el mismo sitio web varias veces,

161
00:31:51.650 --> 00:32:00.459
Lawrence Wold: hacemos solicitudes con los registros del dominio o las compañías de alojamiento web como GoDaddy, Namecheap.

162
00:32:00.770 --> 00:32:07.979
Lawrence Wold: Otra cosa que hacemos es identificar las señales de alarma. Voy a compartir algunas de las señales de alarma,

163
00:32:08.500 --> 00:32:22.200
Lawrence Wold: después de revisar cientos de sitios web soy muy bueno identificando algunas señales de alarma y así, reportándolas a las compañías de alojamiento web, hemos podido cerrar más de 100 sitios web.

164
00:32:23.590 --> 00:32:39.420
Lawrence Wold: Estas son algunas de las señales de alarma habituales con las que se enfrentan en un sitio web fraudulento. Sería bueno que el público pueda decirles esto a sus amigos "Déjame revisar este sitio web en el que crees que estás ganando mucho dinero.

165
00:32:39.440 --> 00:32:45.859
Lawrence Wold: Quizás podemos hablar con alguien de la policía para saber si es un sitio web real o no".

166
00:32:46.370 --> 00:32:48.069
Lawrence Wold: La primera señal de alarma

167
00:32:48.960 --> 00:33:05.439
Lawrence Wold: siempre es que hay tasas de retorno imposibles. Esta captura de pantalla es de un sitio web que cerré. Prometía un retorno diario del 3%. Y si saben de un poco de finanzas o

168

00:33:05.740 --> 00:33:18.300
Lawrence Wold: de inversiones, el 3% diario es imposible. Eso durante un año es una tasa de retorno del 1000%. Eso persuade a las personas para que envíen su dinero.

169
00:33:19.270 --> 00:33:32.399
Lawrence Wold: Otra señal de alarma muy frecuente en los sitios web fraudulentos es que no hay información de contacto. Los sitios web reales tendrán un teléfono, una dirección física, un correo electrónico.

170
00:33:32.540 --> 00:33:38.539
Lawrence Wold: Si hay un correo electrónico en uno de estos sitios web fraudulentos, a menudo es algo raro como

171
00:33:38.650 --> 00:33:43.910
Lawrence Wold: una cuenta de Gmail o de Yahoo.

172
00:33:43.990 --> 00:34:03.060
Lawrence Wold: Las de Gmail son las más frecuentes, pero podrían tener una interfaz de usuario rara como PayFundssfx@gmail. Las URL de compañías reales como Coinbase y Cryptocurrency o Crypto.com y Binance siempre estarán escritas como @Coinbase, por ejemplo.

173
00:34:03.970 --> 00:34:23.920
Lawrence Wold: Los sitios web fraudulentos casi siempre tratarán de que sus víctimas se comuniquen por WhatsApp, Telegram o funciones de chat. Rara vez tratan de comunicarse por correos electrónicos reales y líneas de teléfono estándar.

174
00:34:25.750 --> 00:34:37.020
Lawrence Wold: La tercera señal de alarma es que estos sitios web fraudulentos toman prestado y roban imágenes y texto de sitios web reales.

175
00:34:37.080 --> 00:34:53.750
Lawrence Wold: Este es un ejemplo de un sitio web cerrado, hice una búsqueda de imágenes a la inversa con Google para identificar esto. Aparece una persona que dice ser James Smith, uno de los nombres más comunes y ubicuos que hay.

176
00:34:53.750 --> 00:35:04.880
Lawrence Wold: Dice que es el CEO. Con una búsqueda de imágenes a la inversa con Google descubrí que en realidad es un autor de Nueva York llamado Michael Helley. Entonces,

177

00:35:04.970 --> 00:35:09.519
Lawrence Wold: este es uno de los ejemplos de las técnicas que usamos.

178
00:35:10.350 --> 00:35:15.870
Lawrence Wold: Otra señal de alarma es que no actualizan activamente los sitios web fraudulentos.

179
00:35:15.880 --> 00:35:30.759
Lawrence Wold: Sé que la fuente es algo pequeña, pero esto es de un sitio web que cerramos no hace mucho tiempo, aunque no habían actualizado su página de noticias desde 2023 o 2022. Esa es una buena señal de alarma, si lo pueden ver.

180
00:35:31.700 --> 00:35:45.889
Lawrence Wold: Otra gran señal de alarma es que casi todos los sitios web dicen que son la plataforma de intercambio principal o el intermediario líder y que tienen millones de clientes. En realidad,

181
00:35:46.140 --> 00:35:56.370
Lawrence Wold: el mercado lo dominan pocas de las principales plataformas de intercambio. Y una de las mejores formas de comprobarlo es en CoinMarketCap.

182
00:35:56.420 --> 00:36:08.729
Lawrence Wold: CoinMarketCap es un sitio web bastante independiente y muestra el volumen de las plataformas de intercambio. Los principales son Binance, Coinbase y OKX.

183
00:36:08.860 --> 00:36:18.220
Lawrence Wold: Si el sitio web falso fraudulento afirma que es una plataforma de intercambio principal y no aparece en CoinMarketCap, definitivamente es una gran señal de alarma.

184
00:36:21.290 --> 00:36:26.449
Lawrence Wold: Algunas de las conclusiones clave que quiero cubrir

185
00:36:26.630 --> 00:36:29.080
Lawrence Wold: son que

186
00:36:30.720 --> 00:36:40.450
Lawrence Wold: si les llega un mensaje aleatorio y quizá es de alguien que conocen o solían conocer, como un amigo de la preparatoria, y el mensaje

187

00:36:40.770 --> 00:37:00.440
Lawrence Wold: afirma que está ganando mucho en ese sitio web y que quiere que se unan a esa persona para invertir, hay una enorme probabilidad de que esa cuenta esté comprometida y de que la persona que les está hablando no sea la persona que conocen.

188
00:37:01.070 --> 00:37:14.249
Lawrence Wold: Pueden decirle a su familia o amigos, especialmente a algunas de las personas más sensibles y susceptibles a caer en estafas, que si reciben una llamada o un mensaje de texto

189
00:37:14.480 --> 00:37:22.829
Lawrence Wold: de una agencia policial o del servicio de jurado, y les dicen que los van a arrestar a menos que

190
00:37:23.150 --> 00:37:29.000
Lawrence Wold: envíen dinero a un ATM para Bitcoin, 100% es una estafa.

191
00:37:29.600 --> 00:37:35.900
Lawrence Wold: Los estafadores son muy buenos, tratan de mantener a la gente en la línea todo el tiempo, pero es mejor advertirles

192
00:37:36.160 --> 00:37:37.559
Lawrence Wold: a las personas.

193
00:37:38.070 --> 00:37:50.750
Lawrence Wold: En realidad, nadie invierte en criptomonedas y esto viene de mi formación en finanzas. Es una especulación, las personas especulan con el oro, con tarjetas de béisbol.

194
00:37:50.750 --> 00:38:04.290
Lawrence Wold: Una verdadera inversión es invertir en una compañía o en bienes raíces, algo que ofrece dividendos o que va a crecer. Las criptomonedas claramente son una especulación y no una inversión.

195
00:38:05.090 --> 00:38:15.840
Lawrence Wold: La policía estamos luchando una batalla difícil. Delitos Cibernéticos del DOJ de California es parte de una coalición a nivel nacional contra las criptomonedas.

196
00:38:15.840 --> 00:38:26.610
Lawrence Wold: Tiene 2,400 miembros en todo el país. Ayudamos con remisiones a agencias locales, ayudamos a identificar

197

00:38:26.740 --> 00:38:32.840
Lawrence Wold: el rastreo en cadena y trabajamos de manera colaborativa.

198
00:38:33.010 --> 00:38:50.329
Lawrence Wold: Desafortunadamente, el 95% de las veces las víctimas no recuperarán nada. Somos la difusión pública, como con esta reunión, vamos a ayudar a la mayor cantidad de personas con quienes podamos hablar y compartir.

199
00:38:50.870 --> 00:38:55.190
Lawrence Wold: Otra conclusión clave es que una vez que el dinero

200
00:38:55.270 --> 00:39:04.990
Lawrence Wold: entra en un ATM para criptomonedas, por lo general desaparece definitivamente. Los estafadores son muy buenos lavando los fondos,

201
00:39:05.040 --> 00:39:17.780
Lawrence Wold: ocultando a dónde fueron. También, una de las naturalezas de las criptomonedas es que pueden dejar los fondos en direcciones sin alojamientos web y tenerlos ahí durante meses.

202
00:39:18.110 --> 00:39:36.080
Lawrence Wold: Hacemos lo que podemos. Ponemos alertas en esa dirección y cuando se mueve, tratamos de seguirla. Es un reto y estamos avanzando un poco, pero va a ser necesaria mucha cooperación y educación para el público.

203
00:39:36.280 --> 00:39:49.509
Lawrence Wold: Los malos, los estafadores casi siempre están en el extranjero. Enjuiciarlos es realmente difícil. Estamos trabajando con

204
00:39:49.630 --> 00:40:05.229
Lawrence Wold: plataformas de intercambio legítimas, con las compañías de alojamiento de sitios web y con webinars, así como con la policía local para tratar de educar a las personas.

205
00:40:05.230 --> 00:40:19.250
Lawrence Wold: Incluso tratamos de trabajar frecuentemente con los dueños de tiendas de autoservicio y licorerías con ATM para criptomonedas para que estén más atentos. Trabajamos con los bancos. A veces las transferencias

206
00:40:19.420 --> 00:40:28.349

Lawrence Wold: se hacen electrónicamente al extranjero y de repente hay personas de 70 y 80 años que hacen una transferencia electrónica

207
00:40:28.350 --> 00:40:40.210
Lawrence Wold: a Vietnam cuando nunca antes habían hecho una transferencia electrónica internacional. Estamos tratando de que los bancos estén un poco más atentos y que ayuden a las personas.

208
00:40:41.570 --> 00:40:51.709
Lawrence Wold: Eso concluye mi sección. Probablemente vamos a comenzar las preguntas y respuestas, y me gustaría volver a presentar a Efraín.

209
00:40:53.050 --> 00:41:03.909
Efraín Botello-Cisneros: Sí, muchas gracias, Lawrence. Lo agradezco mucho. También gracias a Sam por una presentación realmente informativa sobre el importante trabajo de la Sección de Delitos Cibernéticos.

210
00:41:03.910 --> 00:41:15.370
Efraín Botello-Cisneros: Los estafadores, como lo mostraron aquí, son muy hábiles, por eso agradezco mucho todas las recomendaciones y las señales de alarma a las que hay que prestar atención, es información muy importante que todos debemos tener en cuenta.

211
00:41:15.400 --> 00:41:34.290
Efraín Botello-Cisneros: Ahora me gustaría invitar al fiscal general adjunto supervisor, Dorian Peters, con el resto de nuestros oradores a la pantalla para comenzar con las preguntas. En este momento, nuestros presentadores revisarán las preguntas que recibimos mediante nuestros registros y también de la caja de preguntas y respuestas de su pantalla, y haremos todo lo posible por responderlas.

212
00:41:34.290 --> 00:41:35.830
Efraín Botello-Cisneros: Si todavía no lo han hecho,

213
00:41:35.830 --> 00:41:44.440
Efraín Botello-Cisneros: envíen sus preguntas mediante la caja de preguntas y respuestas de su pantalla. Si tienen una pregunta para un presentador en específico, díganlo en su pregunta.

214
00:41:44.440 --> 00:42:01.760
Efraín Botello-Cisneros: También tengan en cuenta que es posible que no podamos responder ninguna pregunta relacionada con investigaciones activas ni sobre otros temas sensibles para proteger la integridad de nuestro trabajo. Gracias por su comprensión. Lo último que señalaré es que si hoy nos acompaña como reportero o está colaborando con la prensa,

215
00:42:01.760 --> 00:42:15.320
Efraín Botello-Cisneros: envíe sus preguntas a agpressoffice@doj.ca.gov. Ahora, le daré la palabra nuevamente al asistente especial del fiscal general, Jamal Anderson, para comenzar con algunas preguntas.

216
00:42:16.110 --> 00:42:34.319
Jamal Anderson: Muchas gracias, Efraín, a usted y a todo su equipo por coordinar este fantástico webinar. Con eso, comenzaremos con algunas preguntas y con una básica que será para Dorian: si se sospecha un delito cibernético,

217
00:42:34.880 --> 00:42:36.090
Jamal Anderson: ¿cómo se reporta?

218
00:42:36.720 --> 00:42:51.849
Dorian Peters: Muy bien, gracias, Jamal y es un gusto estar aquí con todos ustedes. Si sospechan de un delito cibernético, básicamente lo reportan como lo harían con cualquier otro delito. El mejor lugar para ir sería a su Departamento de Policía local.

219
00:42:52.750 --> 00:42:55.069
Dorian Peters: También hay un sitio web

220
00:42:55.070 --> 00:43:19.460
Dorian Peters: que administra el FBI llamado IC3. Básicamente, se llama Centro de Quejas de Delitos Cibernéticos. Ese es otro lugar realmente importante para reportar delitos. El FBI trabaja mucho en delitos cibernéticos y usa los reportes de ese sitio web para poder encontrar víctimas de delitos y, a veces para relacionar casos. A veces,

221
00:43:19.460 --> 00:43:21.960
Dorian Peters: si hay una estafa o

222
00:43:21.960 --> 00:43:27.829
Dorian Peters: una víctima, esta podría no ser la única y el FBI puede usar esos datos para armar los casos.

223
00:43:27.830 --> 00:43:47.530
Dorian Peters: Algo en lo que quiero enfatizar es que en estas investigaciones el tiempo es muy importante y probablemente no es recomendable reportarlo, al menos al inicio, con la oficina del fiscal general, porque no somos la primera línea de respuesta. A lo que me refiero es que no tenemos un centro de comunicación

224

00:43:47.530 --> 00:43:59.790
Dorian Peters: para enviar a un oficial a su casa en unos pocos minutos u horas. Recibimos los reportes, investigamos, procesamos, pero las cosas que hacemos suelen tomar

225
00:43:59.800 --> 00:44:12.750
Dorian Peters: semanas, meses e incluso a veces, años. Pero si son víctimas de un delito, necesitan ayuda de inmediato, así que asegúrense de comunicarse con su Departamento de Policía local que pueda responder y ayudarlos inmediatamente.

226
00:44:14.020 --> 00:44:28.630
Jamal Anderson: Gracias, Dorian. Una pregunta relacionada que creo que quizás coincide con su respuesta anterior es ¿qué medidas deben tomar las víctimas tan pronto como se den cuenta de que han sido víctimas de una transferencia electrónica fraudulenta? Sé que lo mencionó.

227
00:44:28.630 --> 00:44:34.660
Jamal Anderson: Las agencias locales son las principales y primeras líneas de respuesta, pero ¿podría ampliar y responder a esta pregunta también?

228
00:44:34.660 --> 00:44:50.740
Dorian Peters: Si son víctimas y hay una transferencia, asumiré que enviaron dinero de alguna manera, entonces agregaré que también deben comunicarse con su institución financiera, no importa cuál sea. Si transfieren dinero usando su banco,

229
00:44:50.740 --> 00:44:57.759
Dorian Peters: Venmo o cualquier servicio que hayan usado, deben comunicarse con ellos. Y nuevamente,

230
00:44:57.760 --> 00:45:02.189
Dorian Peters: quiero destacar el hecho de que el tiempo es muy importante.

231
00:45:02.190 --> 00:45:25.289
Dorian Peters: Algunas de estas aplicaciones pueden transferir dinero de inmediato y algunas en minutos. Si hacen una transferencia electrónica, puede pasar en minutos, horas o días, dependiendo del tráfico, de su banco y sus políticas. El hecho clave es que deben actuar inmediatamente. Esto no es algo que se deba pensar mucho.

232
00:45:25.340 --> 00:45:37.950
Dorian Peters: Si ya están por irse a dormir, y piensan "Lo reportaré por la mañana", no está bien. Esto es algo para lo que deben empezar a hacer

esas llamadas, comunicarse con la policía y con sus instituciones financieras de inmediato.

233
00:45:38.290 --> 00:45:41.400
Dorian Peters: El tiempo es esencial.

234
00:45:43.680 --> 00:45:54.830
Jamal Anderson: Gracias, Dorian. Tenemos una pregunta que llegó sobre las estafas de SEO. Me pregunto si puede hablar un poco sobre lo que es una estafa SEO y

235
00:45:55.080 --> 00:45:57.689
Jamal Anderson: cómo evitarla.

236
00:45:58.260 --> 00:46:12.249
Dorian Peters: SEO significa optimización para motores de búsqueda y por lo general se refiere a que las personas escriben cosas en sus sitios web para que aparezcan al principio de una búsqueda específica de Google.

237
00:46:12.420 --> 00:46:19.129
Dorian Peters: En resumen, de cierto modo las personas pueden usarlo para tratar de convencerlos de entrar a un sitio al que no tenían intenciones de entrar.

238
00:46:19.220 --> 00:46:24.090
Dorian Peters: Por ejemplo, digamos que usan los servicios bancarios de Bank of America.

239
00:46:24.090 --> 00:46:49.069
Dorian Peters: Alguien podría crear un sitio web en el que en el código oculto que no ven podrían poner Bank of America, finanzas, dinero y todos estos términos, así cuando busquen su banco a veces es posible que Bank of America no sea el primer resultado o que este sitio fraudulento esté en la primera página de los resultados de Google, y si entran a esa página, muchas veces tratarán de duplicar el sitio de Bank of America.

240
00:46:49.070 --> 00:46:54.250
Dorian Peters: Así pensarán que están iniciando sesión en Bank of America, pero en realidad están iniciando sesión en el sitio web del estafador.

241
00:46:54.250 --> 00:47:19.110
Dorian Peters: Si lo hacen, deben saber que cualquier información que proporcionen en realidad será para el estafador, no para su banco. Si pasara eso, deben comunicarse con su banco inmediatamente y asumir que

cualquier información que pongan en ese sitio web fraudulento está comprometida. Deben tratar de deshacer lo que puedan. Cambiar la contraseña, los números de cuenta, los números de la tarjeta de crédito,

242
00:47:19.110 --> 00:47:22.609
Dorian Peters: si los pusieron en uno de estos sitios web. Entonces,

243
00:47:22.610 --> 00:47:25.470
Dorian Peters: esas son las estafas por SEO y es lo que vemos.

244
00:47:26.760 --> 00:47:44.140
Jamal Anderson: Muchas gracias. Lawrence, tenemos una pregunta en la línea de su presentación y es sobre una persona que se encuentra con, amigos o familia presuntamente, que les dicen a las personas que inviertan en Bitcoin. Podrían tener una oficina física

245
00:47:44.450 --> 00:47:55.520
Jamal Anderson: y las personas hacen lo que esta persona les sugiere, y están obteniendo ganancias. Supongo que la pregunta de manera general es ¿cómo diferenciar entre las

246
00:47:55.520 --> 00:48:04.650
Jamal Anderson: personas reales que participan en este asunto de las Bitcoin y las estafas de las que habló? ¿Puede hablar de eso un poco más?

247
00:48:05.440 --> 00:48:07.199
Lawrence Wold: Es una buena pregunta.

248
00:48:07.520 --> 00:48:23.239
Lawrence Wold: Creo que algo de eso tiene que ser con validación de que la persona vendiendo tenga licencia o ¿los están animando a que

249
00:48:23.700 --> 00:48:31.640
Lawrence Wold: inviertan algo de dinero en criptomonedas en un portafolio equilibrado o está siendo muy concentrado?

250
00:48:32.190 --> 00:48:35.469
Lawrence Wold: Y también

251
00:48:35.490 --> 00:48:54.770
Lawrence Wold: quizás también deba hablar con la policía sobre hacer una revisión de antecedentes de esta persona o comprobar si tiene alguna denuncia previa. Como dije, es el viejo oeste. Frecuentemente no se puede saber en quién confiar

252
00:48:54.880 --> 00:49:13.890
Lawrence Wold: en línea. Pero la aceptación gradual de las criptomonedas como un activo va a crear más de estos problemas. Entonces, si las personas quieren comprar criptomonedas, deben hacerlo de una plataforma de intercambio legítima.

253
00:49:14.350 --> 00:49:23.060
Lawrence Wold: Coinbase, por ejemplo, tiene sede en EE. UU. aquí en California y hay más plataformas de intercambio

254
00:49:23.570 --> 00:49:29.780
Lawrence Wold: legítimas en las que pueden poner su dinero, si eligen tomar ese riesgo.

255
00:49:31.290 --> 00:49:34.210
Victoria Terry: ¿Puedo agregar un poco a eso?

256
00:49:34.540 --> 00:49:59.529
Victoria Terry: Veo la tendencia de las denuncias sobre criptomonedas que recibe nuestra oficina, yo las proceso y veo muchísimas de estas en las que la persona piensa que es una plataforma real, en la que ve resultados, ganancias de dinero y que puede retirarlo, así es como juegan con ustedes. Los hacen pensar que es un sitio real y dos semanas después

257
00:49:59.530 --> 00:50:14.879
Victoria Terry: o un mes después, no importa el tiempo, de repente todo el dinero desaparece, no pueden acceder a él, les piden más dinero y es así cómo esas plataformas pueden jugar con ustedes para hacerlos creer que es legítima, cuando en realidad no lo es.

258
00:50:16.430 --> 00:50:28.190
Jamal Anderson: Gracias, Sam. Quiero seguir con ese tema. Hablaste un poco sobre el AB821. ¿Puedes explicar la función que cumple el AB821 en cómo comenzó el trabajo en delitos cibernéticos en el DOJ?

259
00:50:28.190 --> 00:50:32.200
Victoria Terry: El AB821 lo

260
00:50:32.280 --> 00:50:48.560
Victoria Terry: aprobó la Asamblea para que coincidiera en trabajo con el programa HTTAP, y ese comité asesor incluyó personas, evidentemente, del Departamento de Justicia,

261

00:50:48.560 --> 00:51:12.010
Victoria Terry: de CDAA, había jefes de policía, la Asociación de Jefes de Policía y Sheriffs, personas de la industria cinematográfica, equipo semiconductor y de Materials International. Era un gran comité que se reunió para asesorar y educar a los policías

262
00:51:12.010 --> 00:51:18.970
Victoria Terry: sobre cómo combatir estos delitos que estaban afectando a los californianos en ese momento.

263
00:51:20.850 --> 00:51:33.490
Jamal Anderson: Muchas gracias. Tenemos una pregunta aquí relativamente directa que es ¿qué hacer cuando se recibe un correo electrónico de estafa y se hace clic en él? Esa pregunta es para ti, Dorian.

264
00:51:33.720 --> 00:51:37.220
Dorian Peters: Si reciben un correo electrónico de estafa

265
00:51:37.220 --> 00:51:56.409
Dorian Peters: y saben que es de estafa, la respuesta obvia es no hacer clic en él. Pero digamos que ya sucedió, hicieron clic en él. Si solo hacen clic, en realidad probablemente no pase nada. Me refiero a que es posible que vean que hicieron clic en él. No es lo ideal, pero tampoco es el fin del mundo.

266
00:51:56.530 --> 00:51:57.640
Dorian Peters: Ahora,

267
00:51:57.780 --> 00:52:14.350
Dorian Peters: si van a un sitio web y comienzan a interactuar con él, ahí es donde pueden meterse en problemas. Deben asumir que cualquier información que pudieran haber puesto en el sitio web al que entraron, ahora es información pública y está en manos de los estafadores que la usarán.

268
00:52:14.420 --> 00:52:22.800
Dorian Peters: Estos tipos de sitios web son los sitios que las personas como Lawrence han estado cerrando

269
00:52:22.800 --> 00:52:38.769
Dorian Peters: con su esfuerzo. Además de avisarnos de ellos, tengan en cuenta que no trabajamos de manera urgente, pero si el sitio web ha estado activo por un tiempo y su intención es cerrarlo, pueden reportarlo a nuestra oficina y podemos trabajar en ello.

270

00:52:38.770 --> 00:52:43.980
Dorian Peters: También pueden reportar sitios web con Google y Microsoft.

271
00:52:44.120 --> 00:52:47.890
Dorian Peters: En Google, el servicio se llama Navegación Segura

272
00:52:47.900 --> 00:53:12.239
Dorian Peters: y en Microsoft se llama Notificar sitio web no seguro. El motivo por el que es muy valioso es porque esencialmente el buscador de todos guarda una lista oculta de los sitios fraudulentos, entonces si lo reportan con Google como un sitio fraudulento, lo que pasará es que cualquier persona que trate de entrar a ese sitio web recibirá una alerta de que otras personas lo han reportado como estafa.

273
00:53:12.240 --> 00:53:16.719
Dorian Peters: Eso puede ser una advertencia que puede ayudar a evitar que otras personas sean víctimas.

274
00:53:18.190 --> 00:53:30.259
Jamal Anderson: Gracias, Dorian. Responderemos una pregunta más y es sobre guardar contraseñas. Obviamente, la mayor parte de esta presentación tiene que ver con mantener segura nuestra información personal.

275
00:53:30.280 --> 00:53:45.119
Jamal Anderson: Tenemos una pregunta muy específica sobre si usar un mecanismo como Apple Keychain, u otros que correspondan para otros dispositivos, es una forma segura de guardar contraseñas, y si hay otras maneras de asegurarse de mantener segura nuestra información.

276
00:53:45.120 --> 00:54:05.169
Dorian Peters: Es una gran pregunta y la respuesta, por lo general, es sí. Hay algunas advertencias que mencionaré, pero por lo general, usar algo como Apple Keychain u otros gestores de contraseñas respetables como Bitwarden, es una buena manera de llevar el seguimiento de hasta 100 contraseñas, porque lo que hacemos con frecuencia es

277
00:54:05.420 --> 00:54:14.179
Dorian Peters: tener una contraseña que usamos para varios sitios web. Y el problema es que si de esos 100 sitios web, hackean el menos seguro,

278
00:54:14.180 --> 00:54:33.130
Dorian Peters: ya tienen la contraseña para las otras 99 cuentas para las que pudimos haber usado ese correo electrónico y contraseña. Es muy importante que usemos contraseñas únicas en todos los sitios web y

cuentas diferentes, y usar un gestor de contraseñas como Apple Keychain es una muy buena forma de hacerlo. Mi advertencia

279
00:54:33.210 --> 00:54:36.109
Dorian Peters: es que ningún sistema es 100% seguro.

280
00:54:36.360 --> 00:54:47.389
Dorian Peters: Apple tiene una muy buena historia de seguridad, pero ninguna compañía puede prometer algo que sea perfecto, e incluso si actualmente es perfecto

281
00:54:47.390 --> 00:55:05.259
Dorian Peters: las computadoras se hacen cada vez más poderosas, entonces incluso quizá algo que no se puede decodificar hoy, una computadora lo podrá hacer en 10 o 20 años, o en el momento que sea. Para equilibrar sí recomiendo algo como Apple Keychain u otros gestores de contraseñas, pero tengan en cuenta que nada es perfectamente seguro.

282
00:55:06.620 --> 00:55:14.760
Jamal Anderson: Gracias, Dorian. Gracias, Sam. Gracias, Lawrence y gracias a todos por participar en estas preguntas y respuestas. Y ahora, volvemos con Efraín.

283
00:55:16.500 --> 00:55:36.190
Efraín Botello-Cisneros: Sí, muchas gracias por acompañarnos hoy en Desmitificando el DOJ sobre la Sección de Delitos Cibernéticos. Esperamos que esta presentación haya sido informativa y útil para ustedes. Los recursos y enlaces mencionados en esta presentación están disponibles en nuestro sitio web, que Ben ha puesto en el chat, y la grabación de esta presentación también estará disponible ahí en breve.

284
00:55:36.190 --> 00:55:43.049
Efraín Botello-Cisneros: Para ver la grabación de esta presentación bajo pedido, también pueden hacer clic en su enlace de participante una vez que este webinar haya finalizado.

285
00:55:43.460 --> 00:55:59.219
Efraín Botello-Cisneros: Les agradeceríamos si pudieran tomarse unos minutos para completar una breve encuesta para decirnos su opinión sobre la presentación de hoy. La encuesta aparecerá en su buscador de Internet cuando salgan del webinar, pero también pueden usar el código QR que aparece en su pantalla si les resulta más fácil.

286
00:55:59.550 --> 00:56:19.430
Efraín Botello-Cisneros: También pondremos el enlace en el chat para su conveniencia. Tómense un momento para completar la encuesta, compartan

sus comentarios para ayudarnos a mejorar para próximos programas. Con eso, les agradezco por asistir, espero que tengan unas maravillosas fiestas, espero que tengan un maravilloso feliz Año Nuevo y esperamos verlos para la próxima en 2026. Muchas gracias.