Comprender el delito cibernético y los delitos económicos

PID_00270257

Thomas Holt

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Thomas Holt

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Marc Balcells Magrans (2019)

Primera edición: septiembre 2019
© Thomas Holt
Todos los derechos reservados
© de esta edición, FUOC, 2019
Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Ninguna parte de esta publicación, incluido el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea este eléctrico, químico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita de los titulares de los derechos.

Índice

Introducción

El desarrollo de ordenadores e internet en los últimos treinta años ha transformado radicalmente el mundo, lo que ha supuesto que la comunicación y el comercio sean inherentemente más fáciles y rápidos. Uno de los beneficios más inmediatos de los ordenadores, los teléfonos móviles e internet radica en el hecho de que ahora podemos obtener información de cualquier persona o cosa en un instante. El hecho de poder adquirir conocimiento de personas, lugares y productos desde cualquier parte del mundo permite en teoría a los humanos estar más informados en todos los aspectos de su vida. Como consecuencia, la conectividad a internet ha aumentado sustancialmente en las naciones occidentalizadas. Aproximadamente, el 85 % de la población de los países miembros de la UE usan internet, con una mayor proporción de uso en Alemania y el Reino Unido (Internet World Stats, 2019). Muchos usuarios de internet gravitan en torno a plataformas de redes sociales, como Facebook y Twitter, que permiten a las personas compartir sus puntos de vista y opiniones sin tener que interactuar físicamente con los demás. De hecho, aproximadamente el 85 % de la población de los países europeos usa Facebook, en comparación con una tasa general de uso del 50 % respecto al resto del mundo (Internet World Stats, 2019).

Del mismo modo, el aumento de las compras en línea a través de plataformas de comercio electrónico como Amazon permite que los consumidores obtengan prácticamente cualquier artículo imaginable en todo el mundo y al mejor precio (Wilson, 2011). Las tasas de compras en línea varían según el lugar, y los países asiáticos tienen un mayor porcentaje de compradores en línea en comparación con la mayoría de los países de la UE (Statista, 2019). La evidencia sugiere que lo habitual es que los consumidores busquen productos en sus teléfonos para luego realizar sus compras mediante su ordenador de mesa o portátil (Chaffey, 2019). Estas transacciones a menudo están habilitadas por los procesadores de pagos financieros que facilitan las transferencias inmediatas de fondos entre cuentas a través de los sistemas bancarios tradicionales, así como por sistemas de pagos de terceros, como Verse.

Los beneficios inherentes a la innovación tecnológica se manifiestan en toda la sociedad, lo que lleva a cambios en el comportamiento humano en línea y fuera de línea. El crecimiento de las comunicaciones mediadas por ordenador, o CMC (en inglés, *computer-mediated communications*), como el correo electrónico y la mensajería instantánea, ha reestructurado las relaciones interpersonales, así como la manera en que interactuamos con las empresas y las agencias gubernamentales. Como resultado, los agentes infractores y criminales han

comenzado a trasladarse a espacios en línea para delinquir, ya sea mediante el uso de CMC o la manipulación directa y la subversión de ordenadores e internet, con el fin de causar daño.

Este material explorará estos fenómenos en detalle y resaltará las características que distinguen los delitos facilitados por la tecnología de aquellos considerados como delitos tradicionales.

1. Definición del uso indebido y uso malicioso de ordenadores

El tremendo potencial que tiene internet para participar en ataques contra su infraestructura, sus datos y sus usuarios exige un conjunto claro de definiciones para comprender estos fenómenos. Con ese fin, la mayoría de los investigadores han aplicado definiciones tradicionales de irregularidades a los entornos virtuales. Por ejemplo, algunos investigadores utilizan la expresión *infracción cibernética* para referirse al uso de la tecnología con el fin de participar en comportamientos que infringen los estándares o valores locales, aunque no son ilegales por ley (Holt, Bossler y May, 2012; Udris, 2016).

Ciberinfracción no ilegal

Un excelente ejemplo de ciberinfracción es el que afecta a personas que consumen contenido pornográfico a través de sitios web y plataformas de redes sociales (Holt y otros, 2013; Shamsudin, Subramaniam y Alshuaibi, 2012). Este comportamiento puede ir en contra de los estándares comunitarios de decencia o moralidad, aunque no es ilegal en sí mismo (Quinn y Forsyth, 2013).

Por el contrario, los actos delictivos son aquellos comportamientos que infringen los estatutos legales codificados y conllevan sanciones a nivel local, estatal, federal o nacional. Muchos países no utilizan la expresión *delito cibernético* en su código penal, sino que identifican las acciones que violan la ley a través de diferentes tecnologías. Esto se debe a la falta de consenso en cuanto al significado de *cibercrimen*, y a su uso en la comunidad de investigadores y profesionales.

Por ejemplo, en la década de 1990 y principios del siglo XXI, los términos *cibercrimen* y *delito informático* se utilizaron para referirse a actividades delictivas relacionadas con la tecnología (Goodman, 1997; Hollinger y Lanza-Kaduce, 1988). Algunos usaron *delito informático* para referirse a actividades en las que el delincuente utilizó un conocimiento especial sobre los ordenadores, mientras que el delito cibernético se usó para aludir a aquellos delitos que se cometieron como resultado de un uso especializado del ciberespacio (Furnell, 2002; Wall, 2001).

A mediados de la primera década de este siglo, prácticamente todos los ordenadores y dispositivos móviles se habilitaron para wifi, lo que llevó tanto a investigadores como a periodistas a abandonar la expresión *delito informático* en favor de *delito cibernético* o *cibercrimen* (Wall, 2007).

Como resultado, el cibercrimen es ahora el término preferido para aludir al uso malicioso de la tecnología.

Otra preocupación creciente entre los encargados de formular políticas radica en la intersección del mal uso de la tecnología con aquella tecnología que sirve a motivaciones ideológicas y políticas, lo que a veces se denomina *ciberterror* (Foltz, 2004; Holt, 2012). Si bien no existe una definición única para *ciberte-*

rrorismo, algunos académicos coinciden en que implica el uso de la tecnología para apuntar a una plataforma digital, un sistema informático o una red (Britz, 2010; Foltz, 2004; Jarvis y MacDonald, 2015). Algunos autores, como Britz (2010), sugieren que el ciberterror también puede incluir el uso de plataformas de comunicaciones para reclutar y radicalizar a otros de acuerdo con su sistema de creencias (véase Britz, 2010). Al mismo tiempo, esta puede ser una definición demasiado amplia, ya que prácticamente cualquier uso de tecnología por parte de terroristas y extremistas podría ser considerado como ciberterror (Jarvis y MacDonald, 2015). Por lo tanto, los investigadores generalmente consideran que el ciberterror es el uso de la tecnología para dañar o alterar la tecnología y los sistemas de comunicaciones en línea con una motivación ideológica (Holt, Stonhouse, Freilich y Chermak, 2019; Jarvis y MacDonald, 2015).

2. Una tipología sobre cibercrimen

El concepto de delito cibernético supone un desafío para el público en general, así como para los investigadores y los encargados de formular políticas, pues son muchos los usos indebidos de la tecnología que pueden darse. Como resultado, algunos autores han argumentado que se necesita una tipología de cibercrimen para ayudar a diferenciar las formas de delincuencia que pueden llevarse a cabo (véase, por ejemplo, Holt, 2013; Wall, 2001). David Wall (2001) creó uno de los marcos más ampliamente citados para clasificar los delitos cibernéticos; sugirió que había cuatro formas de delito: 1) ciberinvasión; 2) ciberfraude y robo; 3) ciberporno y delitos de pornografía, y 4) ciberviolencia. Estas categorías reflejan delitos tanto instrumentales como expresivos, así como la utilización de diferentes habilidades y conocimientos tecnológicos para cometer dichos delitos.

El primero de ellos, la **ciberinvasión**, se refiere a los intentos de cruzar los límites invisibles de las propiedades en espacios virtuales, de manera similar al robo y allanamiento de viviendas (Wall, 2001).

> Por ejemplo, el uso de contraseñas para proteger el correo electrónico y las cuentas de redes sociales, así como las redes wifi y los sistemas informáticos son intentos claros de evitar que un recurso sea mal utilizado por personas que no están autorizadas a emplear estos servicios. Estos usuarios que no están autorizados y que deben intentar adivinar la contraseña o utilizar otros medios más sofisticados están técnicamente traspasando una barrera clara de control al intentar obtener acceso sin permiso del operador.

Se cree que muchos de los actos asociados con la ciberintrusión provienen de *hackers* que utilizan sus conocimientos de hardware y software para obtener acceso a sistemas informáticos, cuentas de correo electrónico y sistemas y servicios protegidos que no son de su propiedad (Furnell, 2002; Jordan y Taylor, 1998). El acto de hackear no es inherentemente ilegal, y puede usarse para proteger los sistemas y poner a prueba su seguridad. Los miembros del público en general no suelen comprender esta diferencia, lo que los lleva a culpar a los *hackers* de delitos graves que afectan a los sistemas financieros y causan daños a los ciudadanos, la industria y el gobierno por igual (véase el módulo 2 para más detalles).

El segundo tipo de ciberdelito según Wall (2001) implica actos de **fraude cibernético y robo**, que pueden ser el resultado directo de varias actividades de ciberintrusión. Esta categoría es muy amplia y abarca una serie de métodos que pueden utilizarse para obtener información, bienes o servicios de personas y redes informáticas. Esto puede incluir el robo de información personal proveniente de bases de datos mediante el uso de técnicas de piratería o herramientas de software malicioso. Además, los delincuentes pueden adquirir de manera fraudulenta información personal directamente de las víctimas mediante el uso de correos electrónicos y perfiles de redes sociales falsos (James, 2005;

Ponemon Institute, 2018). Independientemente del método que emplee, el delincuente puede usar estos datos para realizar transacciones financieras no autorizadas o venderlos para su uso (Holt y Lampke, 2010; Yip y otros, 2013).

El robo cibernético también incluye varias formas de adquirir propiedad intelectual sin pagar al titular original de los derechos de autor o al creador de contenido, generalmente a través de medios no autorizados de copia de medios digitales (Gopal, Saunders, Bhattacharjee, Agrawal y Wagner, 2004).

Piratería digital

La piratería digital supone grandes costes para el propietario de la propiedad intelectual, ya que, según diversos informes, la industria discográfica de Estados Unidos pierde más de doce mil millones de dólares cada año solo por descarga ilegal de música (Siwek, 2007). La venta de productos falsificados también se incluye en esta tipología; estos productos falsificados se venden fácilmente a través de minoristas en línea a consumidores que pueden no darse cuenta de su procedencia real (Kennedy, 2016; Wall, 2010).

El auge de la tecnología también ha extendido un tercer tipo de delito relacionado con el **ciberporno y el contenido pornográfico**. Esta categoría incluye específicamente la creación y difusión de contenido sexualmente explícito a través de proveedores legítimos, así como de los creadores de contenido *amateur* que utilizan herramientas de captura de audio y vídeo de alta definición (Lane, 2000). Además, hay una gran cantidad de servicios sexuales que operan a través de plataformas de comunicación mediadas por ordenador, como las prostitutas que se anuncian en sitios web como Backpage (Cunningham y Kendall, 2013; Finn y Stalans, 2016). Por último, la tecnología ha sido utilizada por pedófilos para adquirir imágenes y vídeos de jóvenes que participan en actos sexuales (Jenkins, 2001; Quayle y Taylor 2002). Una pequeña proporción de delincuentes también utiliza la tecnología para embaucar a menores de edad y conseguir el contacto y abuso sexual fuera de línea (Wolak, Finkelhor y Mitchell, 2004; Wolak, Mitchell y Finkelhor, 2003).

La última categoría señalada por Wall incluye actos de **violencia cibernética** mediante los que un delincuente utiliza la tecnología para enviar, recibir o acceder a materiales nocivos, hirientes o peligrosos en línea. Estos delitos afectan tanto a los jóvenes como a los adultos, ya que las redes sociales permiten que la información sobre otros se observe en tiempo casi real y permanezca por siempre en línea (Finkelhor, Mitchell y Wolak, 2000; Finn, 2004; Hinduja y Patchin, 2009; Holt y Bossler, 2009). La naturaleza del delito varía desde el acoso, la amenaza o los mensajes sexuales enviados por correo electrónico, texto u otra forma de CMC (Bocij, 2004; Finn, 2004). El contenido de un mensaje también puede dirigirse a un solo individuo o a grupos sociales más amplios que pueden asociarse más comúnmente con grupos de odio y violencia política en el mundo real (Hegghammer, 2013; Holt, 2012; Weimann, 2011). Además, aquellos *hackers* y agentes motivados ideológicamente pueden atacar los espacios virtuales para participar en actos de terrorismo o extremismo en plataformas en línea (véase Holt y otros, 2019).

3. Reconocer las motivaciones tras los delitos cibernéticos

La diversidad de delitos que se clasifican como ciberdelitos pone en cuestión por qué los actores se han adaptado a los espacios virtuales. La primera razón, y la más directa, sería la facilidad con la que se puede utilizar la tecnología para infringir la ley. Los ordenadores, los teléfonos móviles y la conectividad a internet son relativamente económicos y fáciles de adquirir en casi cualquier país del mundo. De hecho, las personas no necesitan tener un ordenador, basta con disponer de acceso a internet en un cibercafé o en una biblioteca pública. Muchos ciberdelitos también requieren una competencia técnica mínima por parte del infractor. Si bien se supone que todos los *hackers* poseen habilidades tecnológicas, muchos de sus ataques se aprovechan de simples fallos de seguridad o de descuidos por parte de los usuarios informáticos (Holt y Bossler, 2016; Ponemon Institute, 2018). Además, ahora existen una serie de proveedores de servicios que ofrecen herramientas y servicios de piratería a cambio de una tarifa (Holt, 2013; Hutchings y Clayton, 2016; Leukfeld y otros, 2017). Por lo tanto, ya no es necesario poseer una gran experiencia informática para llevar a cabo un delito cibernético si simplemente se puede pagar a otra persona para cometer ataques cibernéticos en su nombre (Holt, Smirnova, Chua y Copes, 2015).

La conexión a internet y la tecnología informática también permiten a los delincuentes atacar con éxito a un gran número de personas, corporaciones y entidades simultáneamente y desde cualquier parte del mundo. En el mundo real, la selección de víctimas está influenciada por las capacidades del delincuente, como su tamaño, su velocidad o el uso de un arma para intimidar a dichas víctimas (Miller, 1998; Wright y Decker, 1997). Incluso en la mejor de las circunstancias, a menudo un delincuente no puede participar físicamente en un ataque a un grupo dada la posibilidad de ser aplacado por sus propias víctimas. Estas características físicas están ausentes en los entornos virtuales, donde los delincuentes tienen tiempo para adquirir cantidades masivas de información sobre individuos y empresas. Después pueden dirigirse a posibles víctimas a través de diferentes puntos de contacto, como el correo electrónico y las redes sociales o mediante diferentes formas de software malicioso en el contexto de la piratería (Cross, 2015; Holt y Kilger, 2012; Whitty, 2013).

> Internet, sin fronteras y bajo demanda, también vuelve absurdas las relaciones físicas y espaciales tradicionales, lo que provoca que las víctimas queden potencialmente vulnerables frente a los delincuentes en todo momento (Yar, 2005).

Otra ventaja del ciberdelito desde la perspectiva del delincuente es que el riesgo de detección y arresto por parte de los agentes policiales es mucho menor que en los espacios físicos. Los delincuentes que participan en delitos personales y de propiedad en el mundo real deben tomar medidas para ocultar su identidad: usar ropa holgada o disimular su rostro (Miller, 1998; Wright y Decker, 1997). En los espacios virtuales, en cambio, hay pocos aspectos directos relacionados con la apariencia física que se pueden identificar en un delincuente, como la altura, el peso y la raza (Wall, 2001). Las personas pueden crear identidades falsas a través del correo electrónico y las redes sociales para ayudar a ocultar su identidad real con respecto a las víctimas (Bocij, 2004). Desde un punto de vista técnico, los delincuentes pueden esconderse fácilmente mediante el uso de servicios proxy que ocultarán información sobre su ubicación física. Algunos incluso utilizan ordenadores ajenos para encubrir más fácilmente sus acciones y complicar el proceso de investigación (Holt, 2013).

No solo es difícil conocer la verdadera identidad del usuario en el ciberespacio, sino que también puede ser extremadamente difícil arrestarlo y procesarlo en caso de que participe en ciertas formas de delito cibernético. Si bien la mayoría de las naciones industrializadas tienen leyes relacionadas con el cibercrimen y el uso indebido de la tecnología, no han establecido relaciones consistentes que permitan investigaciones transnacionales de delitos (Brenner, 2008; Wall, 2007).

Ejemplo

Por ejemplo, las personas que viven en Rusia y que atacan sistemas informáticos en Estados Unidos pueden estar violando las leyes de ambos países. Sin embargo, no existe una relación de extradición entre estas dos naciones, lo que hace difícil llevar a ese individuo a Estados Unidos para ser juzgado por sus delitos. Estos factores pueden provocar que los delincuentes ataquen selectivamente determinados países dado un menor riesgo percibido de detección (Brenner, 2008).

Los desafíos presentes en la detección e investigación del delito cibernético también afectan a la probabilidad de que las víctimas denuncien sus experiencias a la policía. Algunas formas de delito cibernético, como la piratería informática, pueden pasar desapercibidas para la víctima hasta que se produce efectivamente el delito. Con el hackeo, las víctimas pueden pensar que la lentitud de su sistema informático o su mal funcionamiento se debe simplemente a un problema técnico (Holt y Bossler, 2013; Ngo y Patternoster, 2011). Los fallos y desperfectos pueden ser síntoma de infecciones de software malicioso o algún otro riesgo informático, por lo que la víctima ya puede haber perdido archivos clave o información confidencial. Los programas de software de protección, como las herramientas antivirus, pueden disminuir la probabilidad de que un ataque se produzca con éxito, aunque solo son efectivos si el usuario sabe cómo utilizar correctamente dicha herramienta en su sistema informático (véase Holt y Bossler, 2016). Si una persona no actualiza el software regularmente o hace que escanee activamente los archivos que intenta descargar, es posible que no sea tan útil para proteger el sistema.

En algunos casos, las víctimas también pueden sentirse demasiado avergonzadas para denunciar el delito a la policía, lo que reduce la probabilidad de que este se investigue. Ciertas formas de fraude en línea requieren que la víctima y el delincuente interactúen de manera directa, por lo que la primera se siente cómplice del delito. Como resultado, pueden llegar a pensar que su experiencia será ignorada por la policía, o que incluso pueden haber cometido algún delito, lo que incrementaría su miedo a informar (Button, 2012; Button, Nicholls, Kerr y Owen, 2014; Cross, 2015). Muchas empresas y grandes organizaciones tampoco están dispuestas a informar que han sido blanco de ciberdelincuentes por la preocupación de que sus clientes puedan perder la fe en ellos y recurrir a los servicios de otros proveedores (Brenner, 2008; Holt, 2003). Del mismo modo, pueden pensar que un ataque reducirá los precios de las acciones y tendrá un impacto negativo en el valor de la empresa (Holt y Bossler, 2016). Esta es la razón por la que muchos sostienen que los ciberdelitos son un problema muy poco reportado en países occidentales.

4. Identificación de un ciberdelito económico

Aunque la tecnología ha influido en prácticamente todos los tipos de delincuencia, este impacto posiblemente sea mayor en los delitos económicos. Los actos de robo cibernético, incluidas diversas formas de fraudes, son efectuados mucho más fácilmente y pueden afectar a una población de víctimas mayor debido al uso de internet y ordenadores (Baker y Faulkner, 2003; Grabosky, 2007). Así, estos delitos son definidos por algunos como delitos cibernéticos, ya que los delitos tradicionales se simplifican mediante el uso de la tecnología (Holt, 2015; Wall, 2007). Al mismo tiempo, los actos de ciberintrusión que se dirigen directamente a sistemas informáticos y repositorios de datos son únicos y brindan a los delincuentes nuevas oportunidades para acceder a información confidencial en todo el mundo. Estos crímenes pueden producir un importante daño económico, y se consideran delitos ciberdependientes, pues no pueden existir sin ordenadores y conexión a internet.

De hecho, el auge de internet y de los ordenadores produjo dos cambios sociales clave que afectan directamente al riesgo de daño económico que puede darse. En primer lugar, los ciudadanos han perdido el control de su información de identificación personal (PII, o *personally identifiable information*), que abarca desde detalles simples como el nombre, la dirección y la fecha de nacimiento hasta información mucho más sensible, como hábitos de compra y preferencias políticas (Byer, 2018; Federal Trade Commission, 2016). La gran cantidad de datos que ahora están disponibles en todos los servicios en línea acerca de un individuo también supone una amenaza para la seguridad pública. Los sitios de comercio electrónico retienen información financiera del cliente para permitir compras inmediatas y la entrega rápida de productos. La seguridad de esta información no está garantizada y depende por completo de los protocolos de seguridad que las compañías establezcan para asegurar la confidencialidad y privacidad de los datos (Brown, 2019).

> Esta información tiene un valor sustancial, ya que puede utilizarse para obtener tarjetas de crédito, préstamos y diversos servicios de agencias gubernamentales (Federal Trade Commission, 2016).

En segundo lugar, las compañías y las redes sociales han monetizado la información sobre los intereses, los comportamientos y la identidad individuales de los consumidores. Esto se debe, en parte, al uso voluntario de redes sociales por parte de la población y a su predisposición para compartir su información a la comunidad mundial (Byer, 2018). Plataformas como Facebook y Twitter ganan dinero al ofrecer servicios de publicidad a empresas y organizaciones que pueden adaptar sus mensajes a un público muy reducido, basado en cono-

cimientos demográficos y de comportamiento obtenidos de sus publicaciones (Byer, 2018; Zunger, 2018). Además, los sitios de comercio electrónico y los minoristas físicos registran el comportamiento de los clientes y ofrecen acceso a su información a cambio de una tarifa de servicios. Como consecuencia, la mayor parte de la información acerca de las vidas de los usuarios dentro y fuera de línea se está fusionando para convertirse en fuentes de datos que las corporaciones pueden estudiar y utilizar para una mejor captación de minoristas y clientes (Zunger, 2018).

Como consecuencia, la tecnología ha permitido una variedad de posibles delitos que comúnmente se conocen como fraude. Los actos de fraude se pueden definir generalmente como la adquisición delictiva de dinero o propiedades de las víctimas mediante el uso de engaños o trampas (véase, por ejemplo, Baker y Faulkner, 2003). Esto último puede suponer una compleja organización, con múltiples delincuentes que coordinan sus fuerzas, o delitos cometidos por un único agente (Button y otros, 2012; Graobsky, 2007). Muchos de estos planes de actuación delictiva implican el uso indebido de los CMC, especialmente el correo electrónico y las páginas web, para así presentar una imagen sugerente que pueda atraer a posibles víctimas. A su vez, la víctima puede proporcionar voluntariamente información personal y detalles financieros a los delincuentes (Button, 2012; Whitty, 2013). Otras formas de fraude no requieren la interacción con las víctimas, ya que el delincuente simplemente ataca las bases de datos financieras corporativas y los sistemas de pago para conseguir información confidencial (James, 2005; Holt y Lampke, 2010).

Estas condiciones han creado un entorno en el que los delincuentes pueden adquirir información confidencial de varias maneras para defraudar tanto a bancos como a proveedores de servicios financieros, solicitar servicios ilegalmente o crear documentos de identidad falsos, como pasaportes y carnés de conducir, para ocultar su verdadera identidad ante las fuerzas policiales.

El público en general, los legisladores y los investigadores a menudo se refieren a estas actividades como fraude o robo de identidad.

El significado y el uso de cada término varía según el lugar, aunque a menudo se emplean indistintamente (Copes y Vieraitis, 2009; Koops, Leenes, Meints, van der Meulen y Jaquet-Chiffelle, 2009). Por ejemplo, los investigadores estadounidenses han definido el robo de identidad como el uso o posesión ilegal de los documentos de identidad de otra persona para cometer, apoyar o participar en actividades ilegales (Allison, Schuck y Learsch, 2005; Copes y Vieraitis, 2009). La Oficina de Estadísticas Judiciales de los Estados Unidos definió el robo de identidad de manera algo diferente, centrándose en sus aspectos económicos, incluyendo «el uso indebido con éxito de una cuenta existente, como una cuenta de tarjeta de débito o crédito, el uso indebido de información personal para abrir un cuenta nueva o el uso indebido de información

personal para otros fines fraudulentos, como obtener préstamos públicos o proporcionar información falsa a la policía en un delito o en un control de tráfico» (Harrell, 2014).

El concepto *robo de identidad* se usa en otros países occidentales para reflejar el uso indebido de la información de identificación personal de otra persona con el fin de obtener dinero, crédito, bienes o servicios en su nombre, así como para habilitar otras formas de fraude financiero (National Fraud Authority, 2013).

Independientemente del lenguaje utilizado, los delitos de identidad son un problema grave en todo el mundo (Button, 2012; Harrell, 2019). De hecho, la amenaza potencial de varias formas de fraude y robo de identidad es alta en toda la Unión Europea debido a la facilidad del cruce de fronteras y a las comunicaciones por internet en general (Button, 2012). Es difícil evaluar el impacto económico de estos delitos dada la falta de denuncias y las dificultades para determinar el número de víctimas, sobre todo cuando se tienen en cuenta los casos de victimización transnacionales (Anderson y otros, 2013; Button, 2012; Internet Crime Complaint Center, 2018).

Un ejemplo de ello se encuentra en los datos recopilados en Estados Unidos que demostraban que hubo más de catorce millones de víctimas de robo de identidad en 2012, con pérdidas variables dependiendo de cómo se usó su información. Por ejemplo, estas víctimas perdieron un promedio de 552 $ cuando el delincuente había utilizado su tarjeta de débito, mientras que si este había hecho uso de la tarjeta de crédito de las víctimas, las pérdidas eran de 1.448 $ (Harrell, 2019).

Como resultado, no podemos ignorar el alcance del daño causado por el delito de identidad y su relación con el fraude y el delito cibernético en general.

Resumen

Mientras los avances tecnológicos continúen transformando la sociedad, también influirán estos cambios en los delitos financieros y en la criminalidad. Este material didáctico proporciona una visión general de las formas más comunes de fraude y robo empleadas por delincuentes en los medios tecnológicos. También se explorarán los factores asociados con la victimización para evaluar el alcance del daño que se produce con estos delitos. Cada módulo se centra en diferentes delitos y formas de cibercrimen económico. Este primer módulo nos introduce en la comprensión del delito cibernético y los delitos económicos relacionados. El módulo 2 examina los actos de ciberintrusión, concretamente la piratería informática y las infecciones de software malicioso. El módulo 3 explora el problema de las tarjetas o el robo y venta de información financiera adquirida a través de diferentes formas de ciberintrusión. El módulo 4 considera los diversos fraudes que pueden darse a través del correo electrónico, incluyendo correos nigerianos y estafas románticas. El módulo 5 detalla las amenazas planteadas por el robo de propiedad intelectual, incluida la falsificación de productos y la piratería digital. El módulo 6 aborda los nuevos ciberdelitos económicos que pueden darse en función del cambio tecnológico.

Bibliografía

Allison, S. F. H.; Schuck, A. M.; Learsch, K. M. (2005). «Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics». *Journal of Criminal Justice* (núm. 33, págs. 19-29).

Anderson, R.; Barton, C.; Böhme, R.; Clayton, R.; Van Eeten, M. J.; Levi, Moore, T.; Savage, S. (2013). «Measuring the cost of cybercrime». En: *The economics of information security and privacy* (págs. 265-300). Berlín/Heidelberg: Springer.

Baker, W. E.; Faulkner, R. R. (2003). «Diffusion of fraud: Intermediate economic crime and investor dynamics». *Criminology* (vol. 41, núm. 4, págs. 1173-1206).

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect your Family*. Westport, CT: Praeger.

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State*. Nueva York: Oxford University Press.

Britz, M. T. (2010). «Terrorism and Technology: Operationalizing Cyberterrorism and Identifying Concepts». En: T. J. Holt (ed.). *Crime On-Line: Correlates, Causes, and Context* (págs. 193-220). Raleigh, NC: Carolina Academic Press.

Brown, E. (2019). «Two thirds of US consumers say government should do more to protect data privacy» [en línea]. *ZDNet* (22 de enero). <https://www.zdnet.com/article/two-thirds-of-us-consumers-say-government-should-do-more-to-protect-data-privacy/>

Button, M. (2012). *Private policing*. Nueva York: Willan.

Button, M.; Nicholls, C. M.; Kerr, J.; Owen, R. (2014). «Online frauds: Learning from victims why they fall for these scams». *Australian & New Zealand Journal of Criminology* (vol. 47, núm. 3, págs. 391-408).

Byer, B. (2018). «Internet users worry about online privacy but feel powerless to do much about it» [en línea]. *Entrepreneur* (20 de junio). <https://www.entrepreneur.com/article/314524>

Chaffey, D. (2019). «E-commerce conversion rates- how do yours compare?» [en línea]. *Smart Insights*. <https://www.smartinsights.com/ecommerce/ecommerce-analytics/ecommerce-conversion-rates/>

Copes, H.; Vieraitis, L. M. (2009). «Bounded rationality of identity thieves: Using offender-based research to inform policy». *Criminology & Public Policy* (vol. 8, núm. 2, págs. 237-262).

Cross, C. (2015). «No laughing matter: Blaming the victim of online fraud». *International Review of Victimology* (núm. 21, págs. 187-204).

Cunningham, S.; Kendall, T. (2013). «Sex for Sale: Online Commerce in the World's Oldest Profession». En: T. J. Holt (ed.). *Crime On-Line: Correlates, Causes, and Context* (2.ª ed., págs. 40-75). Raleigh, NC: Carolina Academic Press.

Federal Trade Commission (2016). *Consumer Sentinel Network Data Book for January - December 2016* [en línea]. <https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf>

Finkelhor, D.; Mitchell, K. J.; Wolak, J. (2000). *Online Victimization: A Report on the Nation's Youth*. Washington DC: National Center for Missing and Exploited Children.

Finn, J. (2004). «A survey of online harassment at a university campus». *Journal of Interpersonal Violence* (núm. 19, págs. 468-483).

Finn, M. A.; Stalans, L. J. (2016). «Understanding how the internet facilitates crime and deviance. *Victims and Offenders* (núm. 11, págs. 501-508).

Foltz, B. C. (2004). «Cyberterrorism, computer crime, and reality». *Information Management & Computer Security* (vol. 12, núm. 2, págs. 154-166).

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. Boston: Addison-Wesley.

Goodman, M. D. (1997). «Why the police don't care about computer crime». *Harvard Journal of Law and Technology* (núm. 10, págs. 465-494).

Gopal, R.; Sanders, G. L.; Bhattacharjee, S.; Agrawal, M. K.; Wagner, S. C. (2004). «A behavioral model of digital music piracy». *Journal of Organizational Computing & Electronic Commerce* (núm. 14, págs. 89-105).

Grabosky, P. N. (2007). *Electronic crime*. Upper Saddle River, NJ: Pearson Prentice Hall.

Harrell, E. (2019). *Victims of Identity Theft, 2016 (NCJ 248991)* [en línea]. <www.bjs.gov/index.cfm?ty=pbdetail&iid=5408>

Hegghammer, T. (2013). «Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice Between Domestic and Foreign Fighting». *American Political Science Review* (núm. 107, págs. 1-15).

Hinduja, S.; Patchin, J. W. (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Nueva York: Corwin Press.

Hollinger, R. C.; Lanza-Kaduce, L. O. N. N. (1988). «The process of criminalization: The case of computer crime laws». *Criminology* (vol. 26, núm. 1, págs. 101-126).

Holt, T. J. (2012). «Exploring the Intersections of Technology, Crime and Terror». *Terrorism and Political Violence* (vol. 24, núm. 2, págs. 337-354).

Holt, T. J. (2013). «Exploring the social organisation and structure of stolen data markets». *Global Crime* (vol. 14, núms. 2-3, págs. 155-174).

Holt, T. J.; Bossler, A. M. (2009). «Examining the applicability of lifestyle-routine activities theory for cybercrime victimization». *Deviant Behavior* (núm. 30, págs. 1-25).

Holt, T. J.; Bossler, A. M. (2013). «Examining the relationship between routine activities and malware infection indicators». *Journal of Contemporary Criminal Justice* (vol. 29, núm. 4, págs. 420-436).

Holt, T. J.; Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Londres: Routledge.

Holt, T. J.; Bossler, A. M.; May, D. C. (2012). «Low self-control, deviant peer associations, and juvenile cyberdeviance». *American Journal of Criminal Justice* (vol. 37, núm. 3, págs. 378-395).

Holt, T. J.; Kilger, M. (2012). «Know your enemy: The social dynamics of hacking» [en línea]. *The Honeynet Project*. <https://honeynet.org/files/Holt%20and%20Kilger%20-%20KYE%20-%20The%20Social%20Dynamics%20of%20Hacking.pdf>

Holt, T. J.; Lampke, E. (2010). «Exploring stolen data markets on-line: Products and market forces». *Criminal Justice Studies* (núm. 23, págs. 33-50).

Holt, T. J.; Smirnova, O.; Chua, Y. T.; Copes, H. (2015). «Examining the risk reduction strategies of actors in online criminal markets». *Global Crime* (vol. 16, núm. 2, págs. 81-103).

Holt, T. J.; Stonhouse, M.; Freilich, J.; Chermak, S. M. (2019). «Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups». *Terrorism and Political Violence* (págs. 1-22).

Hutchings, A.; Clayton, R. (2016). «Exploring the provision of online booter services». *Deviant Behavior* (vol. 37, núm. 10, págs. 1.163-1.178).

Internet Crime Complaint Center (2018). *Federal Bureau of Investigation Internet Crime Complaint Center (IC3)* [en línea]. <https://www.ic3.gov/about/default.aspx>

Internet World Stats (2019). «Internet Users by Country, 2019» [en línea]. <http://www.internetlivestats.com/>

James, L. (2005). *Phishing Exposed*. Rockland: Syngress.

Jarvis, L.; Macdonald, S. (2015). «What is cyberterrorism? Findings from a survey of researchers». *Terrorism and Political Violence* (vol. 27, núm. 4, págs. 657-678).

Jenkins, P. (2001). *Beyond Tolerance: Child Pornography on the Internet*. Nueva York: New York University Press.

Jordan, T.; Taylor, P. (1998). «A sociology of hackers». *The Sociological Review* (núm. 46, págs. 757-780).

Kennedy, J. (2016). «Proposed Solutions to the Brand Protection Challenges and Counterfeiting Risks Faced by Small and Medium Enterprises (SMEs)». *Journal of Applied Security Research* (vol. 11, núm. 4, págs. 450-468).

Koops, B. J.; Leenes, R.; Meints, M.; van der Meulen, N.; Jaquet-Chiffelle, D. O. (2009). «A typology of identity-related crime: Conceptual, technical, and legal issues». *Information, Communication & Society* (vol. 12, núm. 1, págs. 1-24).

Lane, F. S. (2000). *Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age*. Nueva York: Routledge.

Leukfeldt, E. R.; Kleemans, E. R.; Stol, W. P. (2017). «Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks». *The British Journal of Criminology* (vol. 57, núm. 3, págs. 704-722).

Miller, J. (1998). «Up it up: Gender and the accomplishment of street robbery». *Criminology* (núm. 36, págs. 37-66).

National Fraud Authority (2013). *Annual Fraud Indicator June 2013* [en línea]. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf>

Ngo, F. T.; Paternoster, R. (2011). «Cybercrime Victimization: An examination of Individual and Situational level factors». *International Journal of Cyber Criminology* (vol. 5, núm. 1).

Ponemon Institute (2018). *2018 Cost of Data Breach Study: Impact of Business Contiunity Management* [en línea]. <https://www.ibm.com/account/reg/us-en/signup?formid=urx-33253&cm_mmc=Search_Google-_-Global+Technology+Services_GTS+Resiliency+Services-_-WW_NA-_-%2Bponemon_b_OV65329&cm_mmca1=000000XA&cm_mmca2=10000924&cm_mmca7=1025197&cm_mmca8=kwd-377907906217&cm_mmca9=_k_EAIaIQobChMIuNrj2bSb4gIViJOzCh2GWgtvEAAYASAAEgK37_D_BwE_k_&cm_mmca10=341628554353&cm_mmca11=b&gclid=EAIaIQobChMIuNrj2bSb4gIViJOzCh2GWgtvEAAYASAAEgK37_D_BwE>

Quayle, E.; Taylor, M. (2002). «Child pornography and the Internet: Perpetuating a cycle of abuse». *Deviant Behavior* (núm. 23, págs. 331-361).

Quinn, J. F.; Forsyth, C. J. (2013). «Red Light districts on blue screens: A typology for understanding the evolution of deviant communities on the internet». *Deviant Behavior* (vol. 34, núm. 7, págs. 579-585).

Shamsudin, F. M.; Subramaniam, C.; Alshuaibi, A. S. (2012). «The Effect of HR Practices, Leadership Style on Cyberdeviance: The Mediating Role of Organizational Commitment». *Journal of Marketing & Management* (vol. 3, núm. 1).

Siwek, S. E. (2007). *The true cost of sound recording piracy to the U.S. economy* [en línea]. <https://www.ipi.org/ipi_issues/detail/the-true-cost-of-sound-recording-piracy-to-the-us-economy>

Statista (2019). «Global markets with the highest online shopping penetration, 2017» [en línea]. <https://www.statista.com/statistics/274251/retail-site-penetration-across-markets/>

Udris, R. (2016). «Cyber Deviance among Adolescents and the Role of Family, School, and Neighborhood: A Cross-National Study». *International Journal of Cyber Criminology* (vol. 10, núm. 2).

Wall, D. S. (2001). «Cybercrimes and the Internet». En: D. S. Wall (ed.). *Crime and the Internet* (págs. 1-17). Nueva York: Routledge.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Weimann, G. (2011). «Cyber-Fatwas and terrorism». *Studies in Conflict & Terrorism* (vol. 34, núm. 10, págs. 765-781).

Whitty, M. T. (2013). «The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam». *British Journal of Criminology* (vol. 53, núm. 4, págs. 665-684).

Wilson, M. (2011). «Accenture survey: Discounters continue to dominate back-to-school shopping» [en línea]. *Chain Store Age* <www.chainstoreage.com/article/accenture-survey-discounters-continue-dominate-back-school-shopping>

Wolak, J.; Finkelhor, D.; Mitchell, K. (2004). «Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study». *Journal of Adolescent Health* (núm. 35, págs. 424).

Wolak, J.; Mitchell, K.; Finkelhor, D. (2003). *Internet Sex Crimes Against Minors: The Response of Law Enforcement*. Washington, DC: Office of Juvenile Justice and Delinquency Prevention.

Wright, R. T.; Decker, S. H. (1997). *Armed Robbers In Action: Stickups and Street Culture*. Boston, MA: Northeastern University Press.

Yar, M. (2005). «The Novelty of "Cybercrime". An Assessment in Light of Routine Activity Theory». *European Journal of Criminology* (vol. 2, núm. 4, págs. 407-427).

Yip, M.; Shadbolt, N.; Webber, C. (mayo de 2013). «Why forums?: an empirical analysis into the facilitating factors of carding forums». En: *Proceedings of the 5th Annual ACM Web Science Conference* (págs. 453-462). ACM.

Zunger, Y. (2018). «Computer science faces an ethics crisis. The Cambridge Analytica scandal proves it». *New York Times* (22 de marzo).