Universitat de les Illes Balears

TRABAJO DE FIN DE GRADO

CIBERDELITOS EN EL SECTOR TURÍSTICO: TIPOLOGÍAS MÁS HABITUALES, PREVENCIÓN Y LA RESPUESTA PENAL ANTE LOS MISMOS

Àngela Colom Torres

Grado de Turismo

Facultad de Turismo

Año Académico 2021-22

CIBERDELITO EN EL SECTOR TURÍSTICO: TIPOLOGÍAS MÁS HABITUALES, PREVENCIÓN Y LA RESPUESTA PENAL ANTE LOS MISMOS.

Àngela Colom Torres

Trabajo de Fin de Grado

Facultad de Turismo

Universidad de las Illes Balears

Año Académico 2021-22

Palabras clave del trabajo:

ciberdelito, personas jurídicas, personas físicas.

Maria Isabel Montserrat Sánchez-Escribano

ÍNDICE

ÍNDICE DE TABLAS

RESUMEN

Los ciberdelitos han estado en aumento estos últimos años a raíz del incremento del uso del internet. Las empresas han pasado a usar las plataformas digitales para realizar sus actividades económicas, a la vez que los usuarios emplean el internet en su día a día. En este trabajo académico se espera explicar con claridad las diferentes tipologías de ciberdelitos y cómo se pueden prevenir.

ABSTRACT

Cybercrimes have been on the rise in recent years as a result of the increased use of the internet. Companies have started to use digital platforms to carry out their economic activities, while users use the internet in their day to day. In this academic work, it is expected to clearly explain the different types of cybercrimes and how they can be prevented.

INTRODUCCIÓN

Este trabajo académico analiza los diferentes tipos de ciberdelitos que más comúnmente tienen lugar en el sector turístico, tanto aquellos que afectan a las empresas como aquellos que afectan a los usuarios. A su vez, examina cuáles son las diferentes medidas que estos están adoptando para prevenir estas conductas o evitar caer en ellas, y, finalmente, expone cuál es la respuesta penal ante estas conductas.

La importancia de este tema radica en la influencia que tuvieron en mí las asignaturas “Nociones básicas del Derecho” y “Derecho público”, ya que, gracias a sus excelentes profesores, ayudaron y enseñaron a esta autora a descubrir y aprender una parte de todo lo que engloba el Derecho. A su vez, esta, la autora, ha querido ir más allá de sus conocimientos e intentar desafiarse a sí misma enfocando este trabajo hacia un ámbito que no es el propio de su grado: el Derecho penal, y más concretamente, el de los ciberdelitos en el sector turístico.

Con este trabajo académico la autora espera ampliar sus conocimientos en la materia. Esta es la principal razón por la que ha escogido esta temática, además de los siguientes motivos: en primer lugar, desea enfocar su carrera profesional hacia el sector turístico, en segundo lugar, porque es conocido que este sector depende en alto grado de la tecnología, y, en tercer y último lugar, porque ha vivido de primera mano algunos de los ciberdelitos que serán objeto de análisis en este trabajo y, a su vez, espera poder ayudar a los usuarios a distinguir las diferentes formas que hay hoy en día de defraudar, para que puedan así evitarlas.

Este trabajo está estructurado en seis apartados; Objetivos y metodología, donde se explica cuáles son las fuentes de información del trabajo y como se ha procesado esta; Estadística, en el cual se explican las empresas que forman parte del sector turístico, el aumento del uso del internet y de los ciberdelitos, tanto de empresas como de usuarios, especialmente durante los tres últimos años. Además, se presentan los resultados de dos encuestas realizadas por la autora dirigidas a empresas dentro del sector turístico y a usuarios de diversas edades. Seguidamente, se identifican los ciberdelitos más comunes en el sector turístico, explicándose en qué consisten, cómo se llevan a cabo y notícias relacionadas con estos. Después, se expondrán las mejores medidas de prevención a adoptar por las empresas y por los usuarios con el fin de evitar ser víctima de un ciberdelito. El quinto punto trata la respuesta jurídica-penal ante los ciberdelitos mencionados, dónde se expondrán qué actos ilícitos se cometen en cada uno de ellos y cómo se penalizan.

OBJETIVOS Y METODOLOGÍA

El objetivo principal de este trabajo consiste en hacer un análisis sobre cómo afectan los ciberdelitos al sector turístico y a sus consumidores. Los objetivos secundarios son:

- Estudiar los ciberdelitos más influyentes dentro del sector turístico y comúnmente usados por los delincuentes.
- Analizar las distintas tipologías de ciberdelitos y cómo se penalizan.
- Sopesar las mejores medidas preventivas a adoptar por empresas y usuarios para evitar los ciberdelitos, o saber cómo reaccionar ante ellos.
- Valorar el conocimiento sobre los ciberdelitos de empresas y consumidores mediante la realización de una encuesta.

Para ejecutar este trabajo se ha buscado información actual en páginas oficiales nacionales y artículos en plataformas digitales tales cómo la biblioteca.UIB.cat y Dialnet, relacionadas con aspectos del sector turístico, los ciberdelitos, la actuación judicial y medidas de prevención. Para el apartado de estadística se han usado datos sacados del Instituto Nacional de Estadística (INE) y de la Fiscalía General del Estado, conjuntamente con artículos del Instituto Nacional de Ciberseguridad (INCIBE) y de la página web oficial de la Guardia Civil.

Los autores que más han ayudado para la ejecución de este trabajo son aquellos que tratan la contextualización y definición de los ciberdelitos, entre ellos los más destacables son Manuel Navarro, Mario Rivera y Franz Gottschalk, Mike Langberg, Elmer Lastdrager y los autores del diario académico "*Human Factors in Phishing Attacks: A Systematic Literature Review*" y su mención en él de Dupont. Para la realización de los apartados de identificación de ciberdelitos y las medidas de prevención han ayudado los artículos publicados por página oficiales tales cómo el Instituto Nacional de Ciberseguridad (INCIBE), la Oficina de Seguridad del Internauta (OSI), eNett International y Google Developers. También se han usado documentos jurídicos extraídos del Boletín Oficial del Estado (BOE) para la realización del apartado "Respuesta jurídica-penal ante los supuestos delictivos". El documento jurídico base en este caso ha sido la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Finalmente, se ha realizado un cuestionario creado únicamente para este trabajo, con el que se ha pretendido analizar si las personas físicas y jurídicas son conscientes de los diferentes tipos de ciberdelitos que se mencionan a lo largo de este trabajo, qué hacen estas para evitarlos y si han sido víctimas de alguno de ellos. La población que formará parte de esta encuesta son aquellos usuarios que usen las redes e internet en su día a día, dentro de un rango de edad amplio (19 a 65 años) y empresas que trabajen dentro del sector turístico. En total ha habido 35 participantes, de los cuales 24 han sido usuarios y los 11 restantes han sido empresas, concretamente, agencias de viajes. La encuesta cuenta con un total de siete preguntas para ambos participantes (usuarios y empresas). Seis de las preguntas son las mismas en ambas encuestas:

1. ¿Sabría definir el concepto de ciberdelito?
2. En caso afirmativo, ¿podría hacer una breve descripción?
3. ¿Ha sido víctima de ciberdelito?
4. En caso afirmativo, ¿ha denunciado?
5. ¿Hace uso de medidas de seguridad para prevenir ser víctima de ciberdelitos?
6. En caso de haber marcado “Sí”, ¿qué medidas de seguridad emplea?

La séptima pregunta es diferente en cada una de las encuestas. A las empresas se les ha preguntado “¿Cree que han aumentado los ciberdelitos en comparación a hace diez años?, mientras que a los usuarios “¿Contratarías un servicio de seguro contra ciberdelitos?”.

ESTADÍSTICA

El sector turístico abarca un amplio abanico de empresas (alojamiento, gastronomía o restauración, actividades recreativas y oferta cultural, Agencias de Viajes (AAVV), Transporte, Tour Operadores (TTOO) y centrales de reserva). Todas ellas, exceptuando las actividades recreativas y la oferta cultural, tienen un alto grado de dependencia tecnológica para el desarrollo de su actividad, y a mayor dependencia, mayor riesgo de amenazas (INCIBE, 2021).

Durante la cuarentena ocasionada por la pandemia mundial de la COVID-19 de 2020, en España muchos comercios, por necesidad, tuvieron que dejar atrás lo tradicional y adaptarse a una nueva etapa de cambios tecnológicos. Un estudio realizado por el INE publicado el 10 de junio de 2020 muestra como aquellos establecimientos que han modificado su funcionamiento durante esta época podrán mantener su actividad económica en un futuro. Concretamente, aún en las empresas del sector de transporte y hotelería que modificaron el funcionamiento de su comercio electrónico, este aumentó solamente un 14,2%. Esto se debe a la paralización total de toda actividad turística durante dos meses ininterrumpidos debido a la pandemia.

Por otro lado, debido al confinamiento por la COVID-19, los usuarios empezaron a consumir mayor internet en su día a día. Estos, al no poder ir a los establecimientos, debido al cierre temporal por la cuarentena, pasaron a comprar a través de comercio electrónico o por correspondencia. Un estudio realizado por el INE en 2021, muestra cómo la cifra de compradores online en los últimos tres meses tiene una tendencia creciente: en 2019, la cifra era del 46,9%, en 2020 era de 53,8% y en 2021 fue de un 55,2%.

Como se ve, el sector turístico hoy en día depende en alto grado de la tecnología, lo que da pie a que ciberdelincuentes puedan cometer sus actos. Por este motivo, el aumento del uso del comercio electrónico por parte de las empresas ha supuesto también el incremento de los ciberdelitos. Gracias a las estadísticas del apartado 8 del Capítulo III de la Memoria de la Fiscalía General del Estado de 2020, titulado Criminalidad Informática, se puede observar que la evolución de los ciberdelitos cometidos a través de las Tecnologías de la Información (TICs) se ha incrementado notablemente, especialmente en lo que

concierne a los fraudes. Por ejemplo, si se atiende a las ciberestafas, en el año 2020 hubo 12.250 procesos judiciales incoados, es decir, un 72,43% del total de denuncias de ciberdelitos. Este índice es significativamente más alto que el de años anteriores, en 2019; 65,51%, en 2018; 61,54%, y en 2017; 55,63%. Aún no existen las memorias ni los análisis para los años 2021 y 2022.

Asimismo, la Guardia Civil expone en su artículo "Para evitar ser víctimas de estafa" que la mayoría de víctimas de estafa no suele formalizar ninguna denuncia por vergüenza y miedo a ser juzgado, lo que dificulta la obtención de cifras reales de la ejecución de este tipo de delito.

Unas encuestas realizadas por la autora reafirman los datos estadísticos mencionados previamente. Las encuestas se han llevado a cabo a empresas del sector turístico y a usuarios. Las empresas tienen constancia al 100% de que son los ciberdelitos mientras que los usuarios sólo un 70,8% ha sabido definirlos ("delitos a través de internet" ha sido la definición más utilizada por ambas partes). Asimismo, aunque los usuarios no tengan pleno conocimiento de los ciberdelitos, sólo 2 de los 24 usuarios (8,3%) que han participado han sido víctimas de ellos y ambos denunciaron los hechos. Por otro lado, 2 de las 11 empresas que han participado han sido víctima de ciberdelito, y otras 2 empresas comentaron a la autora que sufrieron intentos de éstos, y ninguno denunció los hechos. En cuanto a medidas de seguridad, vemos una clara diferencia, un 90,1% de las empresas usan ciberseguridad (antivirus, pasarela de pagos segura, etc.) y también les ayuda a evitar ciberdelitos su experiencia en el sector. Por el contrario, un 79,2% de los usuarios no utilizan medidas de seguridad al navegar por internet o realizar compras on-line. Aún así, aquellos usuarios que hacen uso de medidas de prevención, suelen utilizar VPN para conectarse a redes wi-fi públicas, antivirus, software, filtros en los correos electrónicos, etc. Cada encuesta constaba de una pregunta única en ella, a las empresas se les preguntó si creen que han aumentado los ciberdelitos en comparación a hace 10 años, y la respuesta ha sido unánime: Sí. Finalmente, la pregunta única en la encuesta de los usuarios ha sido "¿Contratarías un servicio de seguro contra ciberdelitos?" dónde un 62,5% de los encuestados ha respondido positivamente, mientras que el 37,5% restante ha negado.

IDENTIFICACIÓN DE CIBERDELITOS EN EL SECTOR TURÍSTICO

En este apartado se estudiarán los ciberdelitos más comunes en el sector turístico. La identificación de estas conductas se realiza de forma muy exhaustiva en la "Guía de recomendaciones para las empresas del sector turístico" proporcionada por el Instituto Nacional de Ciberseguridad (INCIBE) y SEGITTUR. Como este trabajo se centra en el sector turístico, en total se explicarán los seis fraudes que más afectan a este. Son los siguientes:

4.1. Skimming

El término *Skimming* proviene del inglés "to skim" que significa "leer con fluidez, deslizar" (Manuel Navarro, 2021). Esta conducta consiste en obtener la información codificada en la banda magnética de la parte trasera de las tarjetas

de crédito o débito para clonarlas. En la presentación que ofrecen Mario Rivera y Franz Gottschalk de “Los Ataques de Skimming en Cajeros Automáticos y Cómo Prevenirlos” se extrae que este delito se produce más comúnmente en cajeros automáticos, pero que, recientemente, ha aparecido el *E-Skimming*, la misma práctica mediante el uso de internet.

Para que el robo en cajeros automáticos se produzca con éxito, los delincuentes necesitan dos herramientas; un “skimmer” y un dispositivo para capturar el PIN. El “skimmer” es un dispositivo que almacena los datos de las tarjetas insertadas en él, el cual usan posteriormente para llegar a descodificar la información confidencial de dentro de la banda magnética de las tarjetas. Estos dispositivos están fabricados para colocarlos sobre la abertura del lector oficial de tarjetas del cajero automático y ocupan toda la superficie de éste, haciendo que sea muy difícil distinguirlos.

Para capturar el PIN, la práctica más usada es la instalación de una “Cámara Estenopeica” que enfoque al teclado para capturar en vídeo el PIN de la víctima. Asimismo, existe el teclado de PIN falso, consiste en alterar el teclado PIN e insertar un dispositivo en éste que capture los PINes de las víctimas. También usan el espiar por encima del hombro cuando las víctimas van a insertar el PIN, poco tecnológico pero muy efectivo. Y la nueva tendencia que usan los delincuentes es ataques de malware; implementan un malware al cajero automático y de esta forma consiguen la información de las tarjetas, además de obtener la habilidad de sacar efectivo y elegir la denominación de billetes que quieran.

Una notícia publicada en El Confidencial, el 24 de febrero en 2020, explica cómo la Policía Nacional arrestó a los líderes de una banda de “skimming”. En el momento del arresto, llevaban consigo 30 tarjetas clonadas y anotaciones con medidas de cajeros automáticos y numeraciones bancarias. La Policía hacía un tiempo que les seguía la pista, y al volver nuevamente a España desde Santo Domingo (República Dominicana) fueron arrestados en el aeropuerto de Madrid-Barajas.

4.2. Phishing y conductas afines

El término *Phishing* se remonta a los años 1995-1996, y surge a raíz de ataques cibernéticos dirigidos a la empresa “America Online Inc.” (AOL), la mayor red nacional de servicios on-line de Estados Unidos. Un hacker había creado un programa, denominado “AOHell”, el cual permitía infiltrarse en la red de la empresa con el fin de robar información confidencial de sus clientes enviando correos o infiltrándose en conversaciones grupales por la red.

En el artículo publicado por Mike Langberg el 8 de septiembre de 1995, encontramos la primera definición de este delito. Este usa el término “fisher” porque el hacker se hace pasar por un agente de la empresa para preguntar a los usuarios sus contraseñas y tarjetas bancarias. Así, la conducta se asemeja a una práctica de “pesca”, ya que consiste en poner un “anzuelo” y esperar a que alguien “pique”.

Años más tarde, en 2014 el autor Lastdrager, a fin de tener una definición clara del término para poder analizarlo y agregar datos sobre esta práctica ilícita para evitar caer en ella, en su artículo "*Achieving a consensual definition of phishing based on a systematic review of the literature*", otorga a este delito una definición consensuada; "el phishing es un acto escalable de engaño mediante el cual se utiliza la suplantación de identidad para obtener información de un objetivo".

Esta definición viene explicada al elegir aleatoriamente veinte palabras (nombres, verbos y adjetivos) de las diversas definiciones de autores como Hutchings and Hayes (2009), Hong (2012), Bose and Leung (2008), Forte (2009), Herzberg (2009) y Amin et al. (2012), y agruparlas en grupos, ya sea por iteraciones, sinónimos o palabras con el mismo significado.

Type	Extracted concept	Occurrence (N)	χ^2	p	
Asset	**Mentioning information***	105	83.27	.00	Consensus
Actor	**Mentions a target***	87	44.61	.00	
Activity	Phishing is digital*	87	32.93	.00	
Activity	Phishing is Internet-based*	84	26.77	.00	
Activity	**Using deception***	79	17.92	.00	
Activity	Communication from target to offender	64	1.99	.16	No consensus
Activity	Communication from offender to target	62	1.07	.30	
Activity	Phishing is a criminal activity	61	0.72	.40	
Activity	**Using impersonation**	60	0.43	.51	
Activity	Phishing uses websites	56	0.01	.93	
Activity	Phishing uses messages	51	1.07	.30	
Actor	Mentions a trusted third party	50	1.50	.22	
Activity	Phishing is fraud*	43	6.45	.01	Consensus
Actor	Mentions an offender*	40	9.64	.00	
Activity	Using persuasion*	30	24.86	.00	
Activity	Mentions the later abuse of information*	22	42.13	.00	
Activity	Related to identity theft*	20	47.16	.00	
Activity	Related to social engineering*	19	49.78	.00	

χ^2-test with df = 1. N = 113. Boldfaced concepts are included in standard. *p < 0.05.

Tabla 4.2.1. Conceptos usados en las definiciones de Phishing. Fuente: Lastdrager Crime Science 2014, 3:9

Así vemos, como hoy en día esta definición prevalece. El Instituto Nacional de Ciberseguridad, define esta estafa siguiendo la definición puesta por Lastdrager:

> "El *phishing* es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico." (INCIBE, 2021).

A raíz del *phishing*, han aparecido otras conductas similares. Como se ha mencionado anteriormente, se denomina *phishing* al fraude que se realiza a través del correo electrónico, pero si el medio utilizado son los mensajes SMS, a este delito se le conoce como *smishing*, y al usar medios como redes sociales, mensajería instantánea o llamadas telefónicas, se está ante un *vishing*. Sin embargo, el objetivo común de estas tres prácticas fraudulentas es

robar información confidencial (tarjetas bancarias, dinero, credenciales de acceso, información delicada de empresas) (INCIBE, 2021).

En 2018, varios clientes de Ryanair fueron notificados vía SMS que la aerolínea ofrecía 2 billetes gratis en conmemoración de su 35 aniversario. El mensaje incluía un enlace que supuestamente redirigía a la supuesta página web de Ryanair, pero la URL era "boletosgratisx" y no "www.ryanair.com". Los clientes avisaron a la misma aerolínea afectada preguntando por el supuesto regalo. Esta desmintió que fuera real, y avisó a sus clientes para que tuvieran precaución. (Maldita.es, 2018)

Uno de los casos más recientes de esta práctica lo han sufrido las Agencias de Viajes miembros de la Asociación Británica de Agencias de Viajes (ABTA). Estas han recibido correos electrónicos en los que el destinatario decía ser la Asociación Internacional de Transporte Aéreo (IATA) en los que, con el asunto de "Circular - Urgente", se adjuntaban varios archivos con un supuesto archivo del lobby aéreo. ABTA ha hecho formalmente una circular, pidiendo precaución frente a este tipo de correos, y recordando que no abran ningún documento ni link imprevisto, ni tampoco intentar contestar estos correos (ABTA, 2022).

4.2.1. Redes inalámbricas: wiretapping, ransomware

Como se ha comentado anteriormente, el incremento de usuarios en las redes tiene una tendencia creciente. Esto ha supuesto que las empresas del sector turístico se modernicen y entre su amplio abanico de servicios y/o productos, hayan empezado a ofrecer una conexión a internet gratuita en sus locales. Esta acción puede ser bien vista por los clientes, al ser una comodidad, por ejemplo, al viajar internacionalmente y no tener una tarjeta SIM en el país de destino.

Por otro lado, existen diferentes conductas fraudulentas en las redes inalámbricas. Dos de la más comunes son: el wiretapping, que consiste en la intercepción ilegal de llamadas telefónicas para la obtención de información confidencial, al igual que pueden suplantar la identidad del receptor de la información o del emisor de esta, y hacer creer a la otra parte que es el legítimo destinatario; y el ransomware, un malware que se introduce en los equipos informáticos de la víctima, a través de enlaces o archivos adjuntos en correos electrónicos o mensajes, "secuestrando" el acceso a la información que se encuentra en los dispositivos infectados. Después de un ataque de ransomware, los delincuentes piden un pago por adelantado a cambio de devolver el acceso a la información a sus víctimas (INCIBE, 2021). Asimismo, encontramos también los denominados "Ataques de fuerza bruta" los cuales consisten en usar todas las contraseñas posibles para la obtención de claves de comunicación o de las que dan acceso a la red wifi. (INCIBE, 2021).

Una de las prácticas más comunes del ransomware es usar los denominados virus "Troyanos". El término fue usado por primera vez en un informe de la Fuerza Aérea EE.UU en 1974 descrito como "*malicious user*" (usuario malicioso), asimismo, el término "Troyano" se hizo popular en la década de los 80'. Hoy en día se conoce como un malware capaz de introducirse en el dispositivo de la víctima (ordenadores de mesa, portátiles, tablets o teléfonos

móviles) sin ser detectado simulando ser actualizaciones de seguridad, descargas de juegos o aplicaciones, archivos o enlaces adjuntos. Estos software maliciosos, a diferencia de los virus, no pueden ser ejecutados por sí solos, necesitan de otro software en el sistema afectado o que sea el mismo usuario que los ejecute sin darse cuenta. El primer virus Troyano en hacerse famoso fue el "AIDS Trojan" en 1989, consistió en mandar disquetes, a través del correo postal, con una supuesta base de datos interactiva referente a la enfermedad del SIDA. Después de 90 ciclos de arranque, cifraba los nombres de archivo del dispositivo, y para que la víctima recuperara sus datos, les exigían enviar entre 200 y 400 dólares a un código postal en Panamá. (ESET, recuperado en 2022).

Miguel Gonazález publicó el 2 de mayo de 2022 en El País el caso más reciente y polémico de wiretapping en España. Las víctimas de tal suceso han sido el presidente del Gobierno de España, Pedro Sanchez, y la ministra de Defensa, Margarita Robles. Los dos sufrieron dos intrusiones en sus teléfonos durante los meses de mayo y junio de 2021 a través el software *Pegasus*, una tecnología imperceptible de origen israelí que puede instalar módulos para leer los mensajes y correos del usuario, escuchar llamadas, hacer capturas de pantalla, registrar claves, extraer información o incluso acceder al historial del navegador. Al presidente le han extraído 2,6 gigabytes y 130 megabytes de información, mientras que a la ministra de Defensa le robaron 9 megabytes. El Ejecutivo no señala ninguna posible autoría por el momento, pero descarta cualquier posibilidad de que el autor sea interno a organismos del Estado.

4.2.2. Pagos Fantasma: estafas informáticas a OTAs y a clientes

Esta modalidad de estafa puede cometerse directamente a empresas o a clientes. Cuando hablamos de esta estafa cometida a agencias de viajes online (OTAs) se conoce como "Pagos Fantasma", mientras que al cometerse a clientes, se le denomina "Fraude de reservas vacacionales".

En el primer caso, este tipo de delito consiste en hacer un supuesto pago, con tarjetas robadas, a una empresa turística para la supuesta reserva de un producto o servicio inexistente o fraudulento. Anthony Hynes, director ejecutivo de eNett International, expone que los estafadores están innovando sus formas de engañar, y que éstas las están dirigiendo a Agencias de Viajes Online (OTAs). Según eNett International los fraudes están costando más de 21.000 millones de dólares a los intermediarios, y se espera que la cifra vaya en aumento (Guest Post, 2018).

En el artículo "The Fake Hotels Phenomenon Targeting OTAs" publicado el 19 de junio de 2018, se distinguen tres nuevas modalidades de pagos fantasma: en la primera, el estafador carga un hotel inexistente en la página web de una Agencia de Viajes Online y reserva habitaciones en ese supuesto hotel, usando tarjetas robadas, la OTA procede a hacer el pago, y para cuando empieza a recibir devoluciones de esos cargos, el hacker ya ha desaparecido con el dinero. El segundo supone la cooperatividad de un hotel y el estafador. El hotel infla los precios drásticamente en una OTA, y esto viene seguido de un auge en las reservas de ese hotel a través del mismo intermediario. Estas reservas las hace un tercero utilizando tarjetas robadas, por tanto, la OTA recibe las

devoluciones de esos cargos, pero el hotel en cuestión presenta documentación al huésped dónde renuncia a cualquier género de responsabilidad por el fraude. Finalmente, el hotel y el estafador se distribuyen las ganancias. Y la tercera ocurre cuando el estafador vende entradas por plataformas sociales a un menor precio por el que las han obtenido a través de una OTA. Cuando es el día de la atracción, la OTA queda desembolsada y el cliente no puede entrar por tener ticket falso y ha sido estafado.

Un caso real de esta práctica, publicado el 24 de enero de 2022 por R.P., ha sido el de la pareja extranjera que estafó más de 8.000 euros a hoteles de Mallorca. Estos dos turistas se dedicaban a simular las transferencias del pago de las estancias, la cual no llegaba a ocurrir.

En el segundo caso, enfocado a usuarios, utilizando a Víctor Malagón, en su artículo publicado el 2/03/2022, expone que están creciendo las denuncias por fraudes en reservas vacacionales en Mallorca. Los estafadores replican o simulan páginas webs de intermediarios, como son Airbnb, Booking, Expedia, utilizando precios similares a los de mercado en estas falsas webs. Las imitaciones de las páginas permiten al usuario completar la reserva, y una vez finalizado el pago, el dinero desaparece juntamente con las páginas webs.

El Instituto Nacional de Ciberseguridad (INCIBE) alerta de el uso excesivo de comparadores de hoteles como son Booking, HomeAway, Trivago, al poderse publicar ofertas de alquiler u hoteles que resultan ser inexistentes. Los estafadores usan imágenes robadas de viviendas y hoteles de zonas muy demandadas.

Víctor Malagón explica como un turista francés fue estafado por una cuantía superior a 4.000 euros al haber reservado nueve noches en un hotel en Mallorca a través de una página web fraudulenta. Francia ha remitido una comisión rogatoria a la Fiscalía de Madrid por ello.

4.2.3. Fraude de maleta

Como informa la Oficina de Seguridad del Internauta (OSI) en un artículo publicado el 14 de diciembre de 2021, el intento de estafa se lleva a cabo por medio de mensajería instantánea y redes sociales (*vishing*).

Consiste en hacerse pasar por un familiar o amigo que ha hecho un viaje al extranjero y, al querer volver, no puede porque supuestamente sus maletas están retenidas en aduanas por problemas en el pasaporte o por el certificado COVID. Para hacer más creíble la estafa, en ocasiones los estafadores hacen llamadas telefónicas haciéndose pasar por un agente aduanero. Cuando ven que han convencido a su víctima, le piden un ingreso de hasta 1.500 euros o superior para poder pagar el coste de aduanas. Una vez han obtenido el ingreso de la cuantía, desaparecen sin dejar rastro. (OSI, 2021).

MEDIDAS DE PREVENCIÓN

En este apartado se expondrán algunas de las medidas recomendadas y utilizadas para evitar los fraudes y otros delitos mencionados en el apartado anterior. Concretamente, se hará referencia a dos tipos de medidas; las medidas de prevención adoptadas por las empresas y las medidas de prevención utilizadas por los usuarios.

5.1. Medidas preventivas a adoptar por las personas jurídicas

Una de las medidas más utilizadas para evitar ciberdelitos en empresas turísticas es el establecimiento de un sistema de ciberseguridad. Como cita José Carrillo et al. en su trabajo "Definición de un Marco de Referencia de Ciberseguridad Empresarial basado en ADM-TOGAF" al autor Xavier Servitja Roca la ciberseguridad "es el conjunto de actividades centradas en mecanismos defensivos y ofensivos empleados para proteger el ciberespacio contra el uso indebido del mismo, defender su infraestructura tecnológica, los servicios que prestan y la información que manejan".

En estos sistemas de seguridad pueden aparecer debilidades. Cómo dice el diario académico "*Human Factors in Phishing Attacks: A Systematic Literature Review*", detrás de un sistema de ciberseguridad seguro siempre encontramos el factor humano, el cual puede fallar en el mantenimiento de éste. Los autores de este diario académico se basan en la teoría "*The Dirty Dozen*" propuesto por Dupont, para exponer una lista de factores humanos a tener en cuenta, con el objetivo de evitar errores de funcionamiento y, por ende, prevenir posibles ciberdelitos. Esta lista está formada por doce puntos:

1. Falta de comunicación dentro de un entorno de trabajo y/o en línea.
2. Complacencia, sentimiento de confianza que puede conducir a falta de conciencia de los peligros potenciales.
3. Distracción.
4. Falta de conocimientos específicos y de experiencia.
5. Falta de trabajo en equipo.
6. Fatiga resultante de períodos prolongados de trabajo y estrés.
7. Falta de recursos para completar una tarea.
8. Presión para cumplir una fecha límite.
9. Falta de asertividad, no poder expresar preocupaciones o ideas.
10. Estrés, por trabajar durante períodos prolongados o problemas exigentes (económicos, familiares, etc.).
11. Falta de consciencia del entorno.
12. Prácticas que se desarrollan con el tiempo que pueden influir en otros comportamientos.

Respecto a los doce puntos mencionados arriba, el Instituto Nacional de Ciberseguridad (INCIBE) junto con SEGITTUR publicaron el 23 de noviembre de 2021 una guía de recomendaciones para las empresas del sector turismo y ocio, con el mismo fin que el anterior, evitar ciberdelitos. Al analizar estas medidas de ciberseguridad, se observa cómo se pueden relacionar con "La

Docena Sucia" mencionadas por Dupont. Algunas de las medidas proporcionadas por esta guía pueden tener más de una correlación con los doce puntos mencionados anteriormente.
A continuación, se incluye una tabla que relaciona las recomendaciones dadas por el INCIBE y SEGITTUR y los doce puntos de Dupont mencionados anteriormente. La tabla se divide en tres columnas, en la primera se encuentran las recomendaciones que vienen dadas en la "Guía de recomendaciones para las empresas del sector turismo y ocio", en la segunda se mencionan los puntos de "La Docena Sucia" con las que estas se pueden relacionar, y, finalmente, en la tercera, se explica la relación entre las dos primeras columnas.

Relación entre recomendaciones para empresas de INCIBE y SEGITTUR y "La Docena Sucia" de Dupont		
Asegurarse correos proceden de un origen confiable	Punto 2 y/o 3 de "La Docena Sucia"	Al tener un sentimiento de confianza podemos olvidarnos de revisar si el remitente es de origen confiable, al igual que si estamos distraídos.
Verificar acción con la fuente que la solicita (ej. cambio cuenta para nómina)	Punto 1 y/o 5 de "La Docena Sucia"	Si un empleado nos pide un cambio de cuenta para la nómina, lo ideal es intentar contactar con él por otro medio de comunicación. No hacer esta revisión demuestra una falta de trabajo en equipo y comunicación.
Tener instalado certificado SSL (protege comunicaciones entre web entidad y dispositivo cliente)	Punto 4 y/o 7 de "La Docena Sucia"	A una empresa puede faltarle el conocimiento para mantener la página web protegida o no tiene recursos para protegerla.
Tener al día actualizaciones de seguridad	Punto 2 de "La Docena Sucia"	Podemos pensar que nuestra seguridad es la mejor y perdernos en el sentimiento de complacencia.
Utilizar contraseñas robustas	Punto 12 de "La Docena Sucia"	Por costumbre podemos empezar a usar contraseñas más fáciles

		para evitar olvidarlas en el tiempo, lo que puede generar un problema de ciberataques a largo plazo.
Realizar copias de seguridad	Punto 1 y/o 3 de “La Docena Sucia”	Si no se comunican entre los empleados la realización de la copia de seguridad (a no ser que sea automática) puede no llevarse a cabo, pudiendo terminar en una pérdida de datos, o el responsable de la copia de seguridad puede distraerse y no realizarla.
Utilizar sistemas de respaldo (permite a la web seguir funcionando en casos de incidente de seguridad o fallo de sistema)	Punto 4 y/o 7 de “La Docena Sucia”	La entidad puede no tener los recursos necesarios ni los conocimientos para proteger bien la página web.
Utilizar sistemas *captcha* (impiden que bots o programas automatizados puedan interactuar con partes de la web corporativa)	Punto 4 y/o 7 de “La Docena Sucia”	La entidad puede no tener los recursos necesarios ni los conocimientos para proteger bien la página web.
Tener instalados entornos de producción y prueba	Punto 4 y/o 7 de “La Docena Sucia”	La entidad puede no tener los recursos necesarios ni los conocimientos para proteger bien la página web.
Asegurar pagos online seguros	Punto 4 de “La Docena Sucia”	La entidad puede no tener los conocimientos para asegurarse de que sus clientes tienen plataformas de pago seguras.
Correcto configuración de la privacidad	Punto 2 y/o 4 de “La Docena Sucia”	Al tener un sentimiento de confianza podemos creer que nuestra

		configuración de privacidad es la adecuada y no serlo, o por el contrario, al no tener los conocimientos necesarios, podemos cometer fallos en esta configuración.
Fomentar la formación y la concienciación de los empleados	Punto 4 y/o 11 de “La Docena Sucia”	El conocimiento y la experiencia pueden ser crucial en una situación donde la empresa se encuentre bajo amenaza, por eso es muy importante formar bien a tus empleados.
Tener precaución con enlaces y archivos adjuntos	Punto 2 de “La Docena Sucia”	El confiarnos puede hacernos errar y no ser conscientes de los peligros inminentes que pueden suponer links o archivos de origen dudoso.

Tabla 5.1.1. Relación entre recomendaciones para empresas de INCIBE y SEGITTUR y “La Docena Sucia” de Dupont. Fuente: elaboración propia

El 21 de marzo de 2020 INCIBE publicó una historia real de un empresario propietario de un hotel en Costa del Sol donde podemos apreciar lo importante que es un sistema de ciberseguridad. A un par de meses de Semana Santa, una empleada de este hotel se percató acerca de varias incidencias en reservas que se habían cancelado debido a fallos relacionados con el procesamiento de los pagos. Decidió poner en conocimiento del propietario del establecimiento, que intuyó que podía ser un intento de ciberdelito e hizo una reunión con todo el personal para revisar minuciosamente todas las reservas que pudieran ser un riesgo para el hotel. Con esta revisión, se dieron cuenta de que un correo mandado por un supuesto cliente dirigido a hacer una reserva para un grupo de viajeros, añadía un cargo extra para pagar un guía que en teoría ya había sido contratado previamente por el cliente. En él se aducía que los clientes no podían pagar directamente al guía y se solicitaba que fuera el hotel el intermediario quien adelantará el pago. Siendo conscientes del ciberdelito que tenían delante, el hotel contestó al correo aceptando hacer el pago siempre que primero recibiera por adelantado una transferencia por el importe de la reserva más el servicio del guía que querían contratar, contestación que nunca tuvo respuesta. Todo quedó en un susto, este hotel consiguió evitar la estafa gracias a la empleada que notificó su sospecha y a la eficacia del programa de gestión de reservas, evitando así un mal mayor.

5.2. Medidas preventivas a adoptar por la persona física

La eficacia de las medidas preventivas de la persona física depende, en muchos casos, de la cautela con la que el usuario abre enlaces o contesta mensajes sospechosos. La Guardia Civil en su artículo “Para no ser víctima de estafa” recalca la importancia de formalizar una denuncia si has sido víctima de este delito. Si la víctima de una estafa por internet resulta ser una persona mayor, suelen tener problemas para recordar los detalles o no saben explicarlo con naturaleza técnica. Aún así, existen medidas de seguridad adoptadas por empresas para proteger la información confidencial de sus clientes, y asegurarse ellas mismas que no están ante un caso de fraude.

Si un sitio web tiene en su URL el acrónimo HTTPS, podemos fiarnos de ésta, al ser un protocolo que garantiza la protección de la integridad y la confidencialidad de los datos comunicados entre los usuarios y el sitio web (OSI, 2020). Esta protección es gracias a los certificados SSL/TLS, un conjunto de los protocolos SSL (*Secure Sockets Layer)* y TLS (*Transport Layer Security*), ya que el protocolo TLS está basado en el SSL (Google Developers, 2022). Los sitios web con los protocolos mencionados anteriormente, usarán para el proceso de pago el protocolo SET (*Secure Electronic Transaction*), el cual asegura la confidencialidad e integridad de la información que se transmite cuando se realiza un pago, el CVV (*Card Verification Value*) que evita compras fraudulentas si el ciberdelincuente sólo tiene el número de nuestra tarjeta, y el AVS (*Address Verification System*) el cual manda una señal de alarma si la dirección de facturación de la compra no coincide con la dirección archivada del banco de la tarjeta utilizada (INCIBE, 2020).

A fin de evitar ser víctima de estos delitos, al igual que las empresas hacen uso de un sistema de ciberseguridad, los usuarios pueden contratar servicios de seguros contra estafas. Un ejemplo nos lo da Caser Seguros, el cual proporciona a potenciales clientes una forma fácil y segura de protegerse del fraude en internet. Caser Legal&Cyberprotección es un seguro que proporciona a sus clientes servicios legales especializados en defensa digital, asistencia y soporte para sus dispositivos y seguridad y monitorización (Caser Seguros, 2021).

Pero no todo el mundo quiere contratar seguros para poder hacer compras en internet. Por eso, en la tabla siguiente hemos hecho una distinción entre ciberdelitos en la primera columna y en la segunda columna se encuentra una descripción de las mejores medidas de prevención.

Distinción de fraudes y mejores medidas de prevención para adoptar por los usuarios	
Skimming	Al ser difícil la distinción de un lector de tarjeta oficial a uno falso, se aconseja inspeccionar regularmente los cajeros automáticos y la implementación de cámaras con circuito cerrado, lector tarjetas jitter, y

	paneles dónde no sea posible añadir un “skimmer”. Los usuarios pueden establecer límites diarios de retirada de efectivo, así cómo activar avisos al sacar efectivo de su tarjeta e ir cambiando el PIN (Rivero, M. & Gottschalk, F. 2014).
Phishing	Este fraude puede darse por diferentes medios; correo electrónico, mensajes SMS, mensajería instantánea, redes sociales y llamadas. Para evitar al máximo estos tipos de fraudes es importante verificar siempre el remitente y el cuerpo del mensaje, una entidad pública o privada no comete errores ortográficos, ya que la atención al cliente es importante para ellas. Si tenemos dudas sobre la veracidad de un comunicado, siempre es preferible llamar a la entidad pertinente y preguntar. Nunca facilitar información delicada, como puede ser DNI o número de tarjetas.
Redes inalámbricas	Este ciberdelito sucede sin que el usuario se de cuenta, no nos envían un correo electŕonico ni un mensaje ni una llamada. Al conectarse a cualquier red inalámbrica se está expuesto a ser defraudado, y más si es una red de Wi-Fi pública, de bar o de restaurante. La organización sin ánimo de lucro AARP, en su artículo “Public Wi-Fi Scams” de 2019 facilita una lista de cosas que hacer frente a estas situaciones. Se puede preguntar a los empleados del establecimiento el nombre de la red y su contraseña, vigilar exactamente que hacemos por la web, hay que intentar evitar llevar a cabo procesos que contengan información delicada. Además, menciona el uso de VPN (Red Privada Virtual), son una herramienta digital que redirige tu tráfico de internet a través de un túnel seguro, ocultando tu dirección IP y encriptando tus datos.

Fraude reservas vacacionales	El artículo que Europapress publicó en 2019 proporciona cuatro consejos que dan los expertos de McAfee, compañía de software especializada en seguridad informática. Para evitar este tipo de fraude, recomiendan entrar en sitios web que el software de seguridad haya autorizado como seguros, al igual que realizar pagos a través de plataformas de confianza, a la vez que sugieren conectarnos a redes con precaución y usar VPN si hay que realizar pagos conectados a una red inalámbrica pública.
Fraude maleta	La Oficina de Seguridad del Internauta (OSI) ofrece cuatro pautas para evitar ser víctima de este fraude. Menciona hacer comprobaciones sobre el usuario con el que interactuamos, si al hablar con esta no nos inspira confianza o nos asaltan dudas, intentar contactar con este supuesto familiar o amigo por otros medios y verificar la situación. Si no se puede contactar con el familiar o el amigo, mejor llamar a la supuesta empresa, por los canales oficiales, donde el contacto supuestamente está retenido y verificar la información. Si al cercionarse de que la situación es falsa, es mejor ignorar los mensajes y bloquear el contacto lo antes posible. (OSI, 2021)

Tabla 5.2.1. Distinción de fraudes y mejores medidas de prevención para adoptar por los usuarios. Fuente: elaboración propia

RESPUESTA JURÍDICA-PENAL ANTE LOS SUPUESTOS DELICTIVOS ANTERIORES

En este apartado se expondrán qué delitos regulados en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, se atribuyen a cada una de los ciberdelitos explicados anteriormente, y cómo se penalizan (pena de prisión y/o multa). A su vez, se explicará más detalladamente qué significa el delito y se analizará una notícia relacionada con cada uno de ellos. Concretamente, se presentan cinco tablas que se distribuyen de la siguiente manera: Los ciberdelitos que incurren sólo un acto ilícito se distribuyen en tres filas; la primera fila es el nombre del ciberdelito, la segunda fila dónde se penaliza y la

tercera fila cómo se penaliza Los ciberdelitos que incurren dos o más actos ilícitos se distribuyen en tres filas y dos o tres columnas, siguiendo la misma distribución de filas que aquellos ciberdelitos con sólo un acto ilícito.

SKIMMING
Robo de información, se penaliza en el *Título X, Capítulo I "Del descubrimiento y revelación de secretos", Artículo 197 y 197 bis del Código Penal.*
Se considera un delito de robo de información cuando el que para descubrir secretos de otro o vulnerar su intimidad, se apodere de sus cartas, mensajes o cualquier otro documento, sin el consentimiento previo. Es delito también la intercepción de las telecomunicaciones de la víctima o usar herramientas de escucha, grabación o reproducción de sonido e imagen en contra de la privacidad de esta.
Pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Tabla 6.1.1. Skimming; qué ciberdelito es y cómo se penaliza. Fuente: elaboración propia

El 3 de enero de 2022, el diario El Mundo publicó la sentencia dada a una banda que manipuló más de 37 cajeros dentro de España. El fiscal los acusó de ser cómplices malayo y por participar en quince hechos delictivos, instalaciones de dispositivos de clonación y sustracciones, y les sentenció a siete años de prisión (El Mundo, 2022).

PHISHING
Suplantación identidad, se penaliza en el *Título XVIII, Sección 4, Capítulo IV "De la usurpación del estado civil", Artículo 401 del Código Penal.* Asimismo, se penaliza también en el *Título X, Capítulo I "Del descubrimiento y revelación de secretos", Artículo 197 y 197 bis Código Penal.*
Se castiga adoptar la identidad civil de otro, sin autorización y lo consiga apoderándose de su correspondencia confidencial o usando medios informáticos, provocando un perjuicio a éste o a un tercero.
Pena de prisión de seis meses a tres años.

Tabla 6.1.2. Phishing; qué ciberdelito es y cómo se penaliza. Fuente: elaboración propia

El 21 de septiembre de 2021, Jornal Noticias informó del fraude que sufrió Cristiano Ronaldo a manos de una agente de viajes. El jugador proporcionó sus datos personales y tarjetas de crédito a dicha empleada, la cual desfalcó 280.000 euros, en tres años, comprando supuestos viajes para el jugador, que nunca fueron realizados, entre febrero de 2007 y julio de 2010. En este caso, la defraudadora ya había sido juzgada en 2017, y fue castigada con 4 años de libertad condicional porque acordó devolver el dinero desfalcado además de abonar un importe mensual a su antiguo jefe por irregularidades durante su estancia en esa agencia, evitando así la pena de prisión.

REDES INALÁMBRICAS	
Daños, se penaliza en el *Título XIII, Capítulo IX "De los daños", Artículo 264 y 264 bis del Código Penal.*	*Extorsión,* se penaliza en el *Título XIII, Capítulo III "De la extorsión", Artículo 243 del Código Penal.*
Este delito ocurre cuando, sin autorización, y de forma grave se borre, dañe, deteriore, altere, suprima o haga que la víctima no pueda acceder a sus datos, programas o documentos informáticos. Además, la práctica ilícita denominada "Ransomware" incurre en otro delito penado en el Artículo 197 bis del Código Penal, al introducirse de forma no autorizada en el sistema informático de la víctima usando medios y herramientas para vulnerar la seguridad de los sistemas (BOE, 1995).	La extorsión empieza en el momento que alguien obliga a otro, con violencia o intimidación a realizar u omitir parte de su patrimonio en perjuicio de éste o de un tercero. Se produce, principalmente, en los casos de ransomware, cuando se solicita a la víctima que pague un rescate por los datos.
Pena de prisión de seis meses a tres años, que puede ascender hasta cinco años	Pena de prisión de uno a cinco años.

Tabla 6.1.3. Redes inalámbricas; qué ciberdelito es y cómo se penaliza. Fuente: elaboración propia

PAGOS FANTASMA
Estafa, se penaliza en el *Título XIII, Capítulo VI, Sección 1.ª "De las estafas", Artículo 249.*
La definición de estafa informática se encuentra reglada en el Artículo 248 del Código Penal en su apartado 2; Aquellos que usando manipulación informática consigan transferirse cualquier activo patrimonial sin que el emisor lo haya consentido, que fabriquen, introduzcan, posean o faciliten programas informáticos destinados a estafas o que utilicen tarjetas de crédito o débito, o cheques de viaje en perjuicio del titular o de un tercero, serán considerados reos de estafa.
La pena de prisión es de seis meses a tres años o multa de uno a tres meses, si la estafa no supera los 400€.

Tabla 6.1.4. Pagos fantasma; qué ciberdelito es y cómo se penaliza. Fuente: elaboración propia

En 2018 se castigó a cinco años y medio de prisión, condena más larga impuesta hasta ahora por estafa, a una agente de viajes de Valladolid, por fugarse a Polonia con más de 82.000 euros de más de un centenar de clientes. Esto ocurrió entre los meses de julio de 2013 y agosto de 2014. La pena impuesta se fijó teniendo en cuenta que la defraudadora cometió un delito continuado de apropiación indebida sumándole las agravantes de reincidencia (en 2012 estuvo año y medio en prisión por hechos similares) y la cuantía estafada. Además, también se le impuso el pago de una multa de 3.600 euros, y el abono de indemnizaciones por los damnificados.

FRAUDE DE MALETA	
Estafa, se penaliza en el *Título XIII, Capítulo VI, Sección 1.ª "De las estafas", Artículo 249.*	*Suplantación identidad,* se penaliza en el *Título XVIII, Sección 4, Capítulo IV "De la usurpación del estado civil", Artículo 401 del Código Penal.*
La definición de estafa informática se encuentra reglada en el Artículo 248 del Código Penal en su apartado 2; Aquellos que usando manipulación informática consigan transferirse cualquier activo patrimonial sin que el emisor lo haya consentido, que fabriquen, introduzcan, posean o faciliten programas informáticos destinados a estafas o que utilicen tarjetas de crédito o débito, o cheques de viaje en perjuicio del titular o de un tercero, serán considerados reos de estafa (BOE, 1995).	Se castiga adoptar la identidad civil de otro, sin autorización y lo consiga apoderándose de su correspondencia confidencial o usando medios informáticos, provocando un perjuicio a éste o a un tercero.
Pena de prisión de seis meses a tres años o multa de uno a tres meses.	Pena de prisión de seis meses a tres años.

Tabla 6.1.5. Fraude de maleta; qué ciberdelito es y cómo se penaliza. Fuente: elaboración propia

CONCLUSIÓN

- Los ciberdelitos van en aumento así cómo va aumentado el uso de internet en el día a día de los usuarios y de las empresas.
- No todos los usuarios son conscientes de qué son los ciberdelitos, pero pocos sufren ataques.
- Al sufrir ciberataques, son pocos los que denuncian (tanto empresas, cómo usuarios).
- Muchos usuarios comprarían un servicio de seguro contra ciberdelitos para sentirse más seguros.

BIBLIOGRAFÍA

Real Academia Española. (s.f.). Estafa. En *Diccionario de la lengua española.* Recuperado en 2022, de https://dle.rae.es/estafa

Ley Orgánica 10/1995, de 25 de noviembre, del Código Penal. *Boletín Oficial del Estado, 281, tit. XIII, cap. VI, sec. I*, de 24 de mayo de 1996. https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

Instituto Nacional de Estadística. (2020). *Porcentaje de establecimientos que habiendo modificado su funcionamiento, lo mantendrán en un futuro (al menos durante los seis próximos meses).* [Conjunto de datos]. INE. https://www.ine.es/jaxi/Datos.htm?path=/COVID/ice/p01/&file=01009.px#!tabs-tabla

Instituto Nacional de Estadística. (2021). *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares.* [Conjunto de datos]. INE. https://www.ine.es/prensa/tich_2021.pdf

Fiscalía General del Estado. (2020). *Memoria 2021, cap. III, sec. 8.* [Conjunto de datos]. https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/index.html

Navarro, M. (2021, 5 septiembre). *Skimming: qué es y como protegerse*. Revista Byte TI. https://revistabyte.es/ciberseguridad/skimming-que-es-y-como-protegerse/

Gottschalk, F., & Rivero, M. (2014, 19 febrero). Los Ataques de Skimming en Cajeros Automáticos y Cómo Prevenirlos. Obtenido de Los Ataques de Skimming en Cajeros Automáticos y Cómo Prevenirlos: https://usa.visa.com/dam/VCOM/download/merchants/Webinar-Preventing-ATM-Skimming-Spanish-021914.pdf

Web Oficial de la Guardia Civil. (s.f.). *Para no ser víctima de estafa.* https://www.guardiacivil.es/es/servicios/consejos/estafa.html

Langberg, M (1995, 8 septiembre). *AOL ACTA TO THWART HACKERS.* Mercury Center Archive Search Results. https://simson.net/clips/1995/95.SJMN.AOL_Hackers.html

Lastdrager, E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science.* **3**:9 https://crimesciencejournal.biomedcentral.com/track/pdf/10.1186/s40163-014-0009-y.pdf

Instituto Nacional de Ciberseguridad. (2021, 22 noviembre). *Phishing, el anzuelo en tu bandeja de entrada.* INCIBE. https://www.incibe.es/aprendeciberseguridad/phishing

Instituto Nacional de Ciberseguridad. (2021, 29 octubre). *TemáTICas Phishing*. INCIBE. https://www.incibe.es/protege-tu-empresa/tematicas/phishing

Association of British Travel Agencies. (2022, 4 febrero). Circular. *Phishing email alert.* ABTA https://www.abta.com/news/phishing-email-alert

Instituto Nacional de Ciberseguridad. (2021, 9 abril). *Ransomware: una guía de aproximación para el empresario*. INCIBE. https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario

Bardají, E. (s. f.). *Pegasus: Qué es y cómo funciona este software de espionaje*. ESED. https://www.esedsl.com/blog/pegasus-que-es-y-como-funciona-este-software-de-espionaje

Gónzalez, M. (2022, 2 mayo). *El Gobierno denuncia que los móviles de Sánchez y Robles fueron espiados con el programa Pegasus*. El País. https://elpais.com/espana/2022-05-02/el-gobierno-informa-que-los-telefonos-de-sanchez-y-robles-han-sido-infectados-con-el-programa-pegasus.html

Travel Weekly Group Ltd. (2018, 19 junio). *Guest Post: The fake hotels phenomenon targeting OTAs*. Travolution. https://www.travolution.com/news/travel-sectors/accommodation/guest-post-the-fake-hotels-phenomenon-targeting-otas/

P, R. (2022, 24 enero). *El truco de dos "turistas" para estafar miles de euros a hoteles de Mallorca*. Preferente.com. https://www.preferente.com/noticias-de-hoteles/el-truco-de-dos-turistas-para-estafar-miles-de-euros-a-hoteles-de-mallorca-315307.html

Oficina de Seguridad del Internatuta. (2021, 14 diciembre). *La estafa de la 'maleta retenida' vuelve a afectar a los usuarios*. OSI. https://www.osi.es/es/actualidad/avisos/2021/12/la-estafa-de-la-maleta-retenida-vuelve-afectar-los-usuarios

Malagón, V. (2022, 6 marzo). Crecen las denuncias por falsas reservas de viajes a Mallorca. Última Hora. https://www.ultimahora.es/noticias/local/2022/03/02/1705553/crecen-denuncias-por-falsas-reservas-viajes-mallorca.html

Desolda, G. et al. (2022, Noviembre). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys, Volume 54, Issue 8, Article No.: 173pp 1–35.* https://doi.org/10.1145/3469886

ESET (2022, 10 mayo). Malware Troyano Características. ESET. https://www.eset.com/es/caracteristicas/malware-troyano/

H. Danilo Jaramillo, S. A. Cabrera, E. M. Abad, V. A. Torres and J. C. Verdúm, "Definition of cybersecurity business framework based on ADM-TOGAF," 2015 10th Iberian Conference on Information Systems and Technologies (CISTI), 2015, pp. 1-7, doi: 10.1109/CISTI.2015.7170391.

Instituto Nacional de Ciberseguridad, SEGITTUR. (2021, 23 noviembre). *Guía de Ciberseguridad para el Sector del Turismo y Ocio*. INCIBE. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-turismo-ocio.pdf

Instituto Nacional de Ciberseguridad (2020, 21 mayo). *Historias reales:a la caza del fraude en las reservas vacacionales.* INCIBE. https://www.incibe.es/protege-tu-empresa/blog/historias-reales-caza-del-fraude-las-reservas-vacacionales

Caser Seguros. (2021, 26 abril). *Cómo protegerte del fraude en internet de forma fácil y segura*. https://www.caser.es/seguros-de-hogar/articulos/proteger-fraude-internet

AARP. (2020, 25 noviembre). *Public Wi-Fi Scams*. https://www.aarp.org/money/scams-fraud/info-2019/public-wifi.html

Europa Press. (2019, 12 junio). *Consejos para evitar estafas al reservas las vacaciones*. europapress.es. https://www.europapress.es/turismo/nacional/noticia-espanoles-admite-haber-sido-estafado-reservar-vacaciones-20190612124435.html

Panda, A. (2021, 21 septiembre). *Cristiano Ronaldo pagou 27 viagens a Tiago sem saber*. Jornal Noticias. https://www.jn.pt/justica/cristiano-ronaldo-pagou-27-viagens-a-tiago-sem-saber-14142225.html

P., R. (2018, 12 junio). *Condena récord a un agente: 5 años de cárcel por estafa*. Preferente.com. https://www.preferente.com/noticias-de-agencias-de-viajes/condena-record-a-un-agente-5-anos-de-carcel-por-estafa-277541.html

Oficina de Seguridad del Internauta. (2020, 27 julio). *HTTPS y certificados digitales, ¿me debo fiar de todos?* OSI. https://www.osi.es/es/actualidad/blog/2020/07/27/https-y-certificados-digitales-me-debo-fiar-de-todos

Google. (2022). *Proteger sitios con el protocolo HTTPS | Centro de la Búsqueda de Google | Documentación* |. Google Developers. https://developers.google.com/search/docs/advanced/security/https?hl=es

Instituto Nacional de Ciberseguridad. (2021, 12 abril). *Consideraciones de seguridad para tu comercio electrónico*. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/consideraciones-seguridad-tu-comercio-electronico

Diario de Valladolid. (2022, 2 enero). *Condena de 7 años de cárcel por clonar en cajeros decenas de tarjetas y luego 'vaciarlas'*. El Mundo. https://diariodevalladolid.elmundo.es/articulo/valladolid/condena-7-anos-carcel-clonar-cajeros-valladolid-decenas-tarjetas-luego-vaciarlas/20220102192006412745.html