República Argelina Democrática y Popular

Ministerio de la Enseñanza Superior y de la Investigación Científica

Universidad AbdelhamidIbnBadis -Mostaganem-

Facultad de Lenguas Extranjeras

Departamento de Lengua Española

Memoria para la obtención de Máster en Lengua y comunicación

Las redes sociales y el riesgo de los delitos informáticos

Caso de estudio: Universidad de AbdelhamidIbnBadisMostaganem, Argelia.

Presentado por:

Dja-bouabdallah Abdessamià

Miembros del jurado

Presidente/a:

Director/a: Sra. Mekkia BELMEKKI (M.C.B)

Vocal:

Año académico: 2019/2020

AGRADECIMIENTOS

Agradezco, primero, a Dios que me ha dado la salud y la fuerza durante la elaboración de mi trabajo de investigación, doy las gracias a mi familia por su apoyo y a mi tutora Dra. Mekkia BELMEKKI por sus esfuerzos, consejos y colaboración. Toda la salud y la bendición a ella y a toda su familia nchalah.

Quería agradecer también a todos mis amigos y amigas que he conocido durante los cinco años de estudio y, por fin, agradezco a mis profesores del departamento de lenguas extranjeras de Oran y de Mostaganem.

Gracias.

DEDICATORIAS

Dedico este modesto trabajo de fin de master a mi familia por el apoyo y el coraje que me han dado y, especialmente, a mi amigo fallecido "Fodil" cuya muerte ha sido una gran pérdida para mí, ¡qué dios le trate con su misericordia nchalah!

Lo dedico también a mis queridos amigos y amigas, mis primos y todas las personas que conozco.

Índice

Internet se puede considerar el líder de los avances tecnológicos producidos en la historia moderna. Se ha convertido una herramienta indispensable y omnipresente en todos los sectores de la vida humana: social, económico, comercial, políticoe intelectual. Por otra parte, genera profundas transformaciones en el dominio comunicativo, elimina las barreras de la distancia y del tiempo, haciendo más simple, rápido y fácil el contacto entre individuos, y particularmente, a través de las redes sociales. Estas plataformas digitales han cambiado nuestra manera de relacionarnos con los demás y nuestra manera de compartir conocimiento e información. Hoy en día, los jóvenes utilizan para todo las redes sociales: dialogar, conocer gente, compartir con ellos noticias, opiniones y eventos, mostrar fotos y vídeos, jugar, etc.

Pero, por mucho que son un gran medio de comunicación e interacción a nivel global, las redes socialesllevan con ellas muchos problemas contra los usuarios a causa del abuso o de un mal uso de las mismas. En efecto, cada información, foto, vídeo, número de cartas bancarias o tarjetas de crédito subidos a una red socialson archivados por los administradores y pueden ser invadidos y robados por parte de otros usuarios. Estas actividades fraudulentas cometidas por medios digitales se conocen por el nombre de delitos informáticos y producen dañosalas personas al nivel social, psicológico y financiero. Las informaciones privadas obtenidas pueden ser publicadas en redes sociales hasta que llegan a miembros de familia y conocidos, lo que afecta la reputación y el honor de la víctima. Por otra parte, el delincuente suele molestar a esta última por medio de amenazas, chantaje o pide dinero a cambio de no publicar los datos adquiridos ilícitamente.

Entonces, cada uno de nosotros, como usuarios de la red, está expuesto a estos crímenes digitales y puede ser alguna vez víctima de un fraude que afecta su identidad, un motivo que nos lleva a arrojar la luz sobre el tema de “las redes sociales y el riesgo de losdelitos informáticos”, tomando como caso de estudio a los estudiantes del departamento de la lengua española de la universidad de Abdelhamid ibn badis Mostaganem. Nuestro interés por el tema se justificatambién por el hecho de ser estos delitos un problema de actualidad y de mayor riesgo en nuestro país. En efecto, Argelia hoy en día está en la cima de los países árabes en el campo de la ciberdelincuecia,el porcentaje de los casos cometidos va creciendo constantemente año tras otro.

Pretendemos, a través de este modesto trabajo poner de relieve la importancia que han adquirido actualmente las redes socialesen la vida cotidiana de los jóvenes, en general, y de los estudiantes en particular, sensibilizar a los internautas de los peligros que puede surgir elmal uso deestas plataformas digitales.Por fin, intentamos orientarles hacia la manera más segura de la utilización de las mismas, conociendo desde dentro todas las opciones y técnicas

que pueden ayudar para evitar caer en la trampa de estos delitos, o a lo menos, reducir sus riesgos.

Para conocer más a fondo el tema en cuestión, es necesario responder a las preguntas siguientes ¿qué son los delitos informáticosy cuáles son sus diferentes tipos y características? ¿Qué debemos hacer para evitar ser uno de las víctimas de estos delitos? ¿Cómo reaccionamos si nuestros datos personales son invadidos o robados de forma ilegal por un ciberdelincuente?

En cuanto a la metodología adoptada es analítica, es decir analizar los datos de los cuestionarios elaborados para saber si los usuarios de internet estánconscientes de los peligros que pueden generar las redes sociales y si saben cómo evitarlos a través de una serie de actuaciones que deben realizar a la hora de navegar.

El presente trabajo consta de dos partes, la primera trata del marco teórico de nuestra investigación y secompone de dos capítulos, el primero,titulado "Las redes sociales y su omnipresencia en la vida personal y profesional de los internautas",trata de las redes sociales, su definición, su origen, su historia, sus tipos y su importancia en la vida del ser humano en todos los sectores incluido el dominio demarketing, de modo que el creciente poder de los consumidores online lleva a diferentes empresas a gestionar sus marcas y su actividades comerciales a través de interactuar de manera directa y efectiva con sus clientes por medio de las diferentes redes sociales como Facebook, Twitter, Instagram, Youtube, LinkedIn, etc. El segundo capítulo lleva como título "Delitos informáticos en las redes sociales"y expone un panorama global sobre este fenómeno: definición, origen y evolución, características, tipos.Tratamos también aquí de los motivos que empujan a los ciberdelincuentes acometer este tipo de crimines. Al final, describimos la naturaleza de estos delitos informáticos en nuestro país Argelia. Cerramos este capítulo, proporcionando una serie de recomendaciones a nuestros estudiantes para evitar ser víctimas de estos delitos.

En cuanto la parte práctica, consta sólo de un capitulo en el que se presenta los resultados dela metodología de la investigación adoptada, analizando los datos de la encuesta destinadaa los estudiantes del departamento de la lengua española. Pretendemos, sobre todo, medir hasta qué punto estos últimos, como usuarios frecuentes de las diferentes redes sociales, están preparados para enfrentar el fenómeno de los delitos cibernéticos y proteger sus datos personales de cualquier intento de fraude ilegal.

Capítulo n° 1

Las redes sociales y su omnipresenciaen la vida personal y profesional delos internautas.

Introducción

Hoy en día, el mundo conoce cambios primordiales con la aparición de Internet, seconvierte en una pequeña aldea donde todos nos conectamos con todos gracias a las redes sociales. Éstas jueguen un papel muy importante en la vida del ser humano en general y de los jóvenes en particular debido a que son herramientas muy útiles que permiten la interacción y la comunicación entre individuos, facilitan el intercambio de ideas, informaciones, imágenes y videos, traspasando asítodas las barreras y dificultades que eran antes tal como la distancia. Por otra parte, nadie puede negar que el mal uso de estas redes tenga muchos inconvenientes y provoca ciertos riesgos, es lo que vamos a tratar en seguida.

1. Definición de las redes sociales

Las redes sociales, según el Diccionario de la Real Academia, son«una plataforma digital de comunicación global que pone en contacto a gran número de usuarios»[1].

Dentro de este contexto, Borja FernándezCamelo[2]define las redes sociales como «*sitios web que permiten a los usuarios entrelazarse para poder comunicarse entre sí, con los amigos que se encuentren dentro de su propia red, en la cual pueden intercambiar fotos, vídeos, mensajes instantáneos, comentarios en fotos*»[3].

Por su parte, Antonio Fumero, investigador de la UPM añade: «*la red(social) muestra una hibridación de ambos extremos: plataformas para crear, editar y compartir contenido generado por el usuario y servicios online para el networking social(contactos) que se consolidan y ofrecen un conjunto de servicios básicos con un valor añadido marginal*»[4].

Otros investigadores insisten en el hecho de que estos espacios virtuales son formados por un grupo de individuos que tienen intereses o actividades en común (amistad, parentesco, trabajo)con el objetivo de comunicarse e intercambiar informaciones, ideas, gustos y opiniones que corresponden a estos intereses o sea que sirven sus labores. En este sentido, Ponce y Maldonado (2016) describen las redes sociales online como:

[1]Disponible en:https://www.rae.es/diccionario-de-la-lengua-espanola/la-23a-edicion-2014
[2] Diplomado en Ciencias Empresariales y técnico superior en ciencias informáticas.Es de Cáceres.
[3] Fernández Canelo, Borja (2010): *Redes sociales: lo que hacen sus hijos en Internet*, San Vicente del Raspeig, Alicante,Editorial Club Universitario, p 96.
[4] Antonio Fumero (2010): «Cultura y vida cotidiana en Iberoamérica, una revisión crítica más allá de la comunicación»,Razón y Palabra, Revista Electrónica en América Latina Especializada en Comunicaciónnúmero 73, Agosto-octubre 2010.

> estructuras sociales compuestas por un grupo de personas que comparten un interés común, relación o actividad a través de internet, donde tienen lugar los encuentros sociales y se muestran las preferencias de consumo de información mediante la comunicación en tiempo real, aunque también puede darse la comunicación diferida en el tiempo, como en el caso de los foros.[5]

Maciá y Gosende (2011) comparten esta misma idea al definir estas redes como «*una plataforma o portal web compuesto por personas o usuarios con intereses comunes que se registran en dicha red social con el objetivo de compartir información personal o profesional, difundiendo todo tipo de contenido, mensajes y noticias*»[6].

2. Tipos de las redes sociales

Actualmente, las redes sociales afectan intensamente nuestra vida cotidiana y profesional, creando nuevas formas de relacionarse con los demás y de compartir conocimiento. Se convierten en herramientas novedosas que utilizamos para todo, esto nos lleva a estudiar más a fondo sus diferentes tipos.2.1. Redes sociales horizontales

Son redes sociales globales que no se dedican ausuarios específicos,todo tipo de individuos tiene el derecho y la oportunidad de acceder a cualquiera de ellas, creando sus propias comunidades y beneficiarse de los servicios que propone. Ejemplos desrtacados de estas redes citamos Facebook, Twitter, Google+, etc. Al contrario, **las redes verticales** son especializadas y se dirigen a un público determinado y se subdividen, por su parte, a varios tipos según sus intereses como veremos en seguida.

2. 1. Redes sociales verticales profesionales

Conocidas también como temáticas. Son un tipo de red social verticalcuyos participantes son profesionales yse enfocan a sectores o empresas que ejercen actividades comunes, se relacionan con objetivos laborales para intercambiar y compartir conocimientos,

[5] Ponce, V. y Maldonado, A. (2016). "Redes Sociales: Definición", recuperado el 9 de julio de 2017 en: http://recursostic.educacion.es//observatorio/web/ca/internet/web-20//1043-redes-sociales?start=1
[6]Maciá, F., y Gosende, J. (2011):*Marketing con redes sociales*,Madrid, Grupo Anaya.

experiencias, valoraciones de producto y servicios que corresponden a la temática y a los intereses de su dominio. La más conocida es LinkedIn.

Se puede incluir aquí las llamadas **redes sociales universitarias** destinadas al público universitario y que permiten a los estudiantes chatear, conocerse y descargar apuntes. Patatabrava es una de las más conocidas.

2.2. Redes sociales de ocio

La temática de este tipo de red social vertical gira en torno a diferentes temas: deporte, música, videojuegos. Wipley o Dogster y Bananit son algunos ejemplos. Existen tambiénredes sociales verticales mixtas quecombinan tanto temáticas profesionales como de ocio, por tanto, son menos formales, por ejemplo, que LinkedIn. Unience es una de las más destacadas.[7]

2.3. Blogging

Un blog es un entorno electrónico estructurado de interacción en el que cualquier persona pueda publicar información, registrando opiniones, historias, artículos y enlaces a otros sitios desde un sitio personal. WordPress y Blogger son los más conocidos. En el ámbito de la Psicología, el más conocido es psicologymente.net, que recibe más de 8 millones de visitas mensuales.

En nuestro país Argelia, en el ámbito educativo, por ejemplo, muchos profesores, universitarios sobre todo, acuden a este medio, creando sus propios blogs para comunicarse con sus estudiantes, ofreciéndoles clases y otras informaciones acerca de la visualización de notas, horarios, citas y encuentros culturales.

Eroles (2010) trata de la importancia de estos blogs en marketing, de modo que, al principio se utilizan sólo por fines personales, pero a partir de 2009, las empresas empiezan a acudir a esta herramienta para comunicarse con sus clientes o sus empleados.[8] Por su parte, Ramos (2017) considera los blogs como una forma más rápida y eficaz que facilita la tarea de las organizaciones y las mantiene más cercanas a sus usuarios[9].

[7]Armando Corbin, Juan (2017): «Los 10 tipos de Redes Sociales y sus características», en: https://psicologiaymente.com/social/tipos-de-redes-sociales
[8]Eroles, J. L. D. G. (2010) : *Internet Marketing 2. 0: captar y retener clientes en la red*, Barcelona, Reverté.
[9]Ramos, J. (2017). Marketing de contenidos. Guía práctica. XinXii.

Por su parte, Manual Moreno (2014) define el blog como un diario electrónico en el cual las empresas registran sus actividades y sus noticias: «*Es el lugar en el que se centralizan todas las acciones de comunicación de la compañía y en el que se almacena todo el contenido que la marca genera en internet*»[10].

2. 4. Microblogging

Estas redes sociales permiten a los usuarios publicar e intercambiar contenidos con una longitud máxima de 140 caracteres tales como frases cortas, imágenes individuales o enlaces de vídeo. Los usuarios pueden suscribirse al contenido de otros usuarios, enviar mensajes directos y responder públicamente, también crear y compartir hashtags para comentar temas o expresar opiniones relacionados a asuntos personales que afectan algunos individuos o públicos que tienen un eco universal. Twitter y Tumblr son los más conocidos.

2. 5. Comunidades de contenido multimedia

El objetivo principal de estos medios sociales es compartir contenido multimedia entre usuarios, permiten cargar y compartir imágenes o vídeos que tratan de todo tipo de dominios y de temas. Los más populares son YouTube (videos), Flickr (imágenes) y Slideshare (presentaciones en Power Point).

2.6. Noticias sociales

Permiten a las personas publicar varias noticias o enlaces a artículos externos y luego los usuarios votan estos artículos. Los ítems que obtienen más votos son los más prominentes yes la comunidad de internautas que decide cuál de las noticias ha logrado el mayor porcentaje de audiencia. Los más populares son Digg y Reddit. Para los usuarios hispanohablantes, existen varios webs con esa misma filosofía como es el caso de Menéame.[11]

[10]Moreno, Manuel (2000- 2014): *El gran libro del Community Manager*, Barcelona , Gestión, p 164.
[11]Armando Corbin, Juan (2017): «Los 10 tipos de Redes Sociales y sus características», en: https://psicologiaymente.com/social/tipos-de-redes-sociales.

3. Origen y evolución de las redes sociales

El origen de las redes sociales es bastante reciente, se puede decir que surgen en 1995 con la creación de "classmates.com" a manos del estadounidense Randy Conrads. Esta red social buscaba reunir ex compañeros de colegio o universidades. En 1997, se creó "SixDegrees",luego, comenzaron a aparecer nuevas redes que pretendían reunir amigos tales como MiGente, AsianAvenue y Match.com, Friendster y a partir del año 2003 ya se había hecho populares otros sitios como LinkedIn y MySpace, con objetivos más específicos.

Como ya se ha explicado en el apartado anterior, existen varios tipos y varios ejemplos de redes sociales, pero nos limitamos aquí a los medios más usados en el mundo actual o sea los que cobran mayor importancia tanto en el ámbito personal o social como en el ámbito empresarial.

3.1. Facebook

Es el líder en la red, apareció en línea el año 2004 por parte de Mark Zuckerbergjunto con sus compañeros con el objetivo de poner en contacto los estudiantes de la universidad Harvard (USA) para compartir resúmenes, noticias trabajos,etc.Después y con la traducción de la red a muchas lenguas extranjeras va a ganar mucha popularidad y gran extensión al nivel mundial.

Facebook permite a sus usuarios crear un espacio digital propio en el cual pueden identificarse a través de su perfil, incorporando datos personales, intereses, aficiones, estudios y gustos. Les permite además establecer relaciones con amigos, familiares o gente nueva y compartir con ellos informaciones, experiencias privadas, eventos, álbumes de fotos, videos y emociones.

La importancia de esta red global radica en la oportunidad que da a las organizaciones y las diferentes administraciones que sea privadas o estatales para comunicarse de forma oficial, inmediata, flexible y rápida con sus usuarios, facilitando así informaciones a la hora. Gálvez (2015) alude a la contribución beneficiosa de Facebook en el dominio empresarial, de modo que permite a las empresas mantener una relación cercana con los clientes de su negocio, creando sus propias páginas de fans[12].

Por otro lado, Facebook se considera una de las mejores posibilidades para realizar una publicidad en línea. Esto se debe al gran número de sus usuarios y la facilidad de acceder

[12]Gálvez Clavijo, Ismail (2015): *Facebook para empresas y emprendedores*, Malaga, IC Editorial.

a esta red, de modo que se puede hacer a través de nuestros móviles sin moverse. En su tesis doctoral, Patricia AlexandraZamora (2016) nos explica el sistema de pago con que cuenta las campañas publicitarias en Facebook y cómo se puede medir el rendimiento de los anuncios a través de la reacción del público hacia ellos, un criterio que ayuda a las empresas para evaluar su actividad productiva:

> La publicidad en Facebook funciona de una forma parecida a Google Adwords, ya que también se basa en el sistema de pago por clico en el pago por cada mil impresiones que reciba tu anuncio. Se marca una impresión cada vez que se muestra el anuncio en Facebook. […] Además se podrá identificar qué anuncios dan mejores resultados, creando varios anuncios con distintas combinaciones de imágenes, enlaces, videos o texto, para que el sistema pueda identificar cuáles funcionan mejor y centrarnos en ellos.[13]

3.2. Twitter

E**s** la red que más representalas llamadas microbloging.Fue creada en el año 2006**,** permite a sus usuarios publicar textos cortos conocidos como "tuits" y seguir a otras personas que les comparten los mismos gustos e intereses y también acercarse a las personas famosas, leyendo sus entradas y publicaciones. Actualmente, esta red social logra popularidad mundial.

Manual Moreno pone de relieve las utilidades que puede presentar esta herramienta para las empresas en marketing y en la difusión o popularidad de las marcas gracias a una interacción exitosa con los clientes o los seguidores (followers): «*Si logramos despertar en el usuario las ganas de interactuar y unirse a la comunidad, mejorará considerablemente la reputación online y la influencia de la marca*»[14]. Esto se explica por la simplicidad de esta plataforma, la brevedad de sus mensajes y la velocidad de la comunicación que propone.

Por su parte, Orihuela (2011) habla de Twitter como un medio de comunicación poderoso que utilizan las empresas para relacionarse con sus usuarios. Para él, si los tuits publicados son más creativos, convincentes, sinceros y expresivos, se garantiza la interacción

[13]Zamora, Patricia Alexandra(2016):*Aplicación web gestora de inteligencia de negocios y el control en la inversión de campañas publicitarias a través de facebook en la empresa Kooper*, (tesis doctoral), Colombia ,Universidad de los Andes, Colombia, pp.27-28.
[14]Moreno, Manuel, op.cit., p 71.

de los clientes y el éxito de los productos.[15]Por esta razón, las empresas tienen que ser muy inteligentes a la hora de seleccionar el contenido de sus mensajes con el fin de llamar la atención de sus seguidores y provocar su interés.

3.3. Instagram

Fue creado por Kevin Systorm y Mike Kreigeren 2010, es una red social y al mismo tiempo una aplicación que utiliza tecnologías como Android, iOS y Windows 10. Permite a sus usuariospublicar y compartir fotografíasy vídeostemporales a su perfil con una duración máxima de permanencia de 24 horas, sonconocidas como "historias"o "stories" en inglés, Éstas se pueden guardar en el perfil permanentemente para que puedan ser vistos, como «Historias destacadas». Instagram posee también un medio de comunicación privado para hablar llamado Instagram Direct (live), una función que permite a los usuarios interactuar a través de mensajes privados con fotos y videos. Estas particularidades hacen de este medio la red social de fotografía más importante del mundo, alcanzando así gran popularidad entre el público joven.

En el dominio de marketing, muchas empresas aprovechan de los servicios particulares de esta red para relacionarse inmediatamente con sus consumidores, publicando fotos de productos, eventos, promociones y novedades. Los usuarios tienen la oportunidad de colgar todos estos contenidos en su perfil, mientras que otros los consultan, comparten y comentan fácilmente, lo que permite la difusión efectiva y veloz de la informaciónque propone la empresa y la popularidad de su marca: «Instagram presentó oficialmente en el año 2016 su herramienta de gestión de perfiles para empresas (similar a la de Facebook), incluyendo un diseño de perfil especial, estadísticas y utilidades de promoción»[16].

[15]Orihuela, José Luis (2011): *Mundo Twitter: Una guía para comprender y dominar la plataforma que cambió la red*, Barcelona, Alienta.

[16]Genbeta social media (2017): «Instagram lanza nuevas utilidades para perfiles de empresas», en Miguel Ángel Sánchez Jiménez (2018) : «Origen y evolución de internet y su desarrollo como entorno de interacción social a través de los medios sociales digitales», disponible en https://www.researchgate.net/publication/326305339.

3.4 .YouTube

YouTube es un sitio web que permite subir, crear y compartir videos. Es el sitio web de su tipo más utilizado en internet, expone una variedad de películas, programas de televisión, vídeos musicales y otros videos de contenidos y temáticas diferente generados por personas conocidos como youtubers. En cuanto al "you" que inicia la denominación es el equivalente de "tú" en español y significa que el contenido es elaborado por el usuario y no por el sitio.Se funda en 2005 en Estados Unidos y en 2006 se convierte en propiedad de Google Inc. Este sitio también permite publicar los enlaces de los diferentes videos publicados a través de las demás redes sociales, lo que facilita la difusión del contenido de video. Por otra parte, muchas empresas prefieren utilizar esta red para lanzar sus productos y servicios debido a la posibilidad audiovisual que ofrece.

3.5. LinkedIn

Es una red social profesional creada por Reid Hoffman a finales de 2002. A diferencia de las redes citadas más arriba,no alcanza tanta notoriedad entre los jóvenes, pero, por otro lado, atrae a muchos otros usuarios que buscan relaciones formales de carácterempresarial o laboral, tal como muestra la profesora Guadalupe Aguado (2015):

> Cuenta a fecha de 2014 con 60 canales diferenciados por temáticas tan diversas como la economía, las finanzas, el deporte, o el entretenimiento, entre otras, de los que catorce superan ampliamente el millón de seguidores y cinco están entre los 3 y 5 millones de seguidores. De esta manera se establece un vínculo estrecho entre los procesos de comunicación y los intereses de los públicos destinatarios.[17]

El perfil utilizado en esta red incluye datos que describen la carrera profesional de los usuarios, lo que les permite formar grupos, comunicarse, interactuar e intercambiar experiencias con aquellos que tienen los mismos intereses y negocios. Por esta razón, esta red

[17]Guadalupe, G. A. (2015): «Inbound marketing en Linkedln para la gestión de marca», La Revista Icono 14, Volumen 13 Nº 1, p 115.

atrae a muchos profesores universitarios que intentan establecer relaciones formales con sus semejantes en otros países y otras universidades.

Por otro lado, LinkedInpermite a las empresas disponer de un perfil profesional, lo que facilita su actividad comercial y publicitaria y la permite estar en contacto con gente especialista en su dominio.La ya citada profesora muestra en un artículo detallado cómo esta red ha ido evolucionando desde su nacimiento en 2002 de red de contactos profesionales hasta convertirse en un espacio de relacionamiento estratégico y gestión de marca. Pone de relieve las diferentes prestaciones de LinkedIn orientadas a la gestión de marca. En efecto, esta red desarrolla un conjunto de técnicas y acciones comunicativas para llegar al consumidor y llamar su atención hacia la marca, lo que se conoce por la metodología del Inbound Marketing.Entre las herramientas para medición de efectividad de contenidosutilizada, la autora cita el caso de Content Marketing Score puesto en marcha en 2014, permite saber qué usuarios únicos han interactuado en las páginas de empresa, grupos, actualizaciones de sus empleados, o en los post de influencers:

> Gracias a esta herramienta la empresa puede saber qué porcentaje de personas ha consultado su contenido, lo ha recomendado, comentado, compartido, o bien ha comenzado a seguir a la empresa. En base a dichos datos se puede elaborar un ranking con resultados de la propia competencia, de forma anónima. Gracias a estos datos las empresas pueden valorar la efectividad de sus estrategias comunicativas en esta plataforma, averiguar qué tipo de acciones son las que registran un mayor alcance y optimizar sus estrategias.[18]

4. Las redes sociales: una moneda de doble cara

Actualmente, las redes sociales se han incorporado de manera notable en la vida de los seres humanos, de modo que se encuentran presentes prácticamente en todos los ámbitos. Uno de los aspectos positivos de la red al nivel de las relaciones humanas y sociales es la vinculación entre las personasa fin de compartir contenidos, interactuar y crear comunidades con intereses y gustos comunes.

[18]Ibid, p 107.

Al nivel empresarial o de marketing, se desarrolla en línea y a gran escala el llamado comercio electrónico que proporciona a las empresas espacios digitales importantes para ejercer negocios, exponer productos y novedades, relacionarse directamente con los clientes y usuarios y hacer propagandas a través de las diferentes campañas publicitarias disponibles.
Por otro lado, y eso es lo más importante para nosotros como estudiantes, algunos sitios como por ejemplo Eduredes tienen objetivos propiamente educativos. En efecto, muchos jóvenes e incluso profesores e investigadores utilizan Internet como una herramienta para realizaractividades estudiantiles, buscar informaciones y fuentes bibliográficas considerables.

Dentro de este contexto, Morales (2011) expresa:

> Las redes sociales influyen de manera positiva, cuando se usan con recato ymoderación, ya que es un medio por el cual te puedes comunicar, no sólo para charlar yplanear eventos sociales, sino también para hacer tareas y trabajos […] Entonces, el problema radica en cómoel estudiante utiliza las redes sociales cómo esto lo afecta a él y a su entorno. Los estudiantes, a pesar de usar las redes para planear eventos sociales y hacer tareas, también, la usan para hacer sentir mal a otras personas y hasta para provocar peleas.[19]

En efecto, un mal uso de la red puede provocar enormes riesgos que afectan negativamente nuestra vida privada y nuestra relación con los demás.Entre estos riesgos aparecen los siguientes:[20]

[19]Morales Pérez, G. (2011): Las redes sociales. Conclusiones de un estudio sobre el grado de conocimiento y utilización por profesionales de la formación, en En Ruiz Palmero, J. ySánchez Rodríguez, J., Buenas prácticas con TIC para la investigación y la docencia. Málaga:Universidad de Málaga.

[20]Joel Dario Coronel Figueroa (2015): *Impacto de las redes sociales en los jóvenes y sus consecuencias*, Monografía para la obtención del título de bachiller, Unidad Educativa Santo Domingo de los colorados bachillerato en ciencias, p15.

4.1. Acceso a contenidos inadecuados

La falta de control en la red y la cantidad de información de que dispone lleva a mucha gente a acceder a contenidos de todo tipo: violentos, sexuales, etc. Esto puede devenir de enlaces publicados o compartidos por otros usuarios o links, avisos, etc.

4.2. Pérdida de privacidad

Cada dato, información, foto, vídeo o archivo subido a una red social pasa a ser parte de los archivos de los administradores. A su vez un mal uso de las redes conlleva a la facilidad de encontrar datos propios, de familiares o amigos. Debemos incluir en esto los hackers que roban contraseñas para manipular información o espiar a las personas.

4.3. Acoso por parte de compañeros, conocidos o desconocidos

Otra desventaja que pueden enfrentar los usuarios es el acoso llevado por compañeros o desconocidos con amenazas e insultos después de haberobtenido fotos e información que se utilizarán por fines maliciosos.

4.4.Posible incumplimiento de la ley

Muchas veces, los usuarios llevan inconscientemente acciones ilegales, los tresIncumplimientos más conocidos son:

- Publicar datos, fotos, vídeos de otras personas, violando su privacidad sin elconsentimiento previo de ellas. Por ejemplo: al subir fotos de nuestro cumpleañossin pedir el permiso de cada una de las personas invitadas o cuyo rostro figura en la foto.
- Hacerse pasar por otra persona, creando un falso perfil y utilizando información obtenida por distintos medios. Ej. Creación cuentas en Facebook y Twitter en nombre deFamosos.
- Incumplimiento de las normas de copyright, derecho de autor y descargas ilegales ade contenidos protegidos.

Conclusión

Recapitulamos diciendo que las redes sociales con su gran número de usuarios se han convertidoen un importante medio social para la interacción humana en todos los dominios de la vida. Sin embargo, por mucho que estas plataformas ofrecen imprescindibles beneficios al ser humano, pueden generarle peligros insoportables. La desventaja más grave es cuando personas desconocidas acceden a o, mejor dicho, invaden datos personales de los usuarios a fin de utilizarlos en maliciosos servicios, causándolesasí grandes problemas. Es lo que se conoce por los delitos informáticos, un punto que trataremos detalladamente en el capítuloprocedente.

Capítulo n° 2

Delitos informáticos en las redes sociales

Introducción

La aparición de internet, como ya se ha explicado en el capítulo antecedente, ha mejorado nuestro modo de vida, pero ha generado también muchos problemas como la adicción, problemas de salud y la violación de la identidad. En este capítulo vamos a arrojar la luz sobre el riesgo más popular que es los delitos informáticos realizados mediante las redes sociales.

1. Definición del delito informático

Hoy en día, el término "delito informático" ha vuelto frecuente y muy popular y es el sinónimo de delito electrónico, ciberdelito, cibercrimen. Se define como toda acción antijurídica realizada en el entorno electrónico o en el espacio digital "Internet" con el objetivo de hacer sentir mal a sus usuarios mediante amenazas o insultos, provocar pérdidas o frenar el uso de sistemas informáticos (delitos informáticos).Estas actividades se cometen mediante el uso deredes, blockchain, computadoras, sistemas informáticos u otros dispositivos de las nuevas tecnologías de información y comunicación.

El Convenio de Ciberdelincuencia del Consejo de Europa, lo define como «*actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, así como el abuso de dichos sistemas, medios y datos*»[1].

Por su parte, Carlos Sarzana lo describe como «*cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo*»[2]. Para Miguel Ángel Davara Rodríguez, otro especialista en el dominio, son delitos informáticos «determinadas acciones y omisiones dolosas o imprudentes, penadas por la ley, en la que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático[3]. Rafael Fernández Calvo lo explica como «*la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos*»[4].

[1] Celebrado en Budapest el 23 de Noviembre de 2001.
[2] SARZANA, Carlos:«Criminalitá e tecnología. Computer Crimes», Rassegna *Penitenciaria* e Criminologica,vol.1 ,n. 1-2, p.59.
[3] DAVARA RODRÍGUEZ, Miguel Ángel (1993):*Derecho informático*, Pamplona: Aranzadi, p. 30
[4]FERNÁNDEZ CALVO, Rafael (1996):« El tratamiento del llamado delito informático en el proyecto de ley orgánica de código penal: reflexiones y propuestas de la CLI (Comisión de Libertades e Informática)», Informática y derecho, n.12, págs. 1149-1162.

Entonces, cualquier tipo de delito informático,automáticamente, tiene relación con la informática por ser llevado a cabo a través o en contra de un dispositivo, un programa o un sistema informático. En este sentido, Ertzaintza dice que la informática constituye a la vez un medio y un fin en el acto de cometer los delitos digitales[5].

2. Historia y evolución del delito informático

Los delitos informáticos existieron mucho más antes de la aparición de Internet. En efecto, los expertos consideran un ataque producido en 1834 como el primer delito informático de la historia. En este ataque, dos ladrones infiltraron en el sistema de telégrafo de Francia con el fin de acceder a los mercados financieros y robar datos necesarios.Luego, en la primera mitad del siglo 20, y precisamente, dos años después del invento del teléfono, unos adolescentes irrumpieron en la fábrica de teléfonos de Alexander Graham Bell y provocaron el caos, redirigiendo las llamadas recibidas unos años después. En 1940, apareció el primer hacker ético llamado Rene Carmille, un francés experto en ordenadores, hackeó el registro de datos Nazi para frustrar sus intentos de registrar y controlar a los judíos.

Entre 1971 y 1993, se registran varios ataques informáticos cometidos generalmente por manipuladores telefónicos(o sea programadores de computadoras obsesionados con las redes telefónicas), personas que manejan sistemas informáticos o por simples empleados en bancos. Los hackeos realizados en este período tienen como objetivos principales: atacar redes de computadoras públicas, banqueras sobre todo, con el fin de transferir dinero a cuentas personales, destruir infraestructuras telefónicas centrales para espiar o simplemente para aprovechar de largas llamadas gratuitas, entrar en sistemas informáticos de gobiernos y de sectores privados para robar datos y venderlos. En 1994, el lanzamiento de World Wide Webpermite que los hackers de sombrero negro muevan su información de producto de los viejos sistemas de tablón de anuncios a sus propios sitios web, lo que hace más rápido, digital y fácil el delito electrónico.Los virus serán enviados a través de conexiones a internet siempre que se visita sitios web cuestionables. Algunos causan que tu computadora funcionara lentamente, otros hacen que la aparición de publicidad invada tu pantalla o la redirija a los sitios pornográficos más asquerosos.A principios del año 2000, con el desarrollo de las diferentes redes sociales en cuyos perfiles los usuarios incluyen sus datos, los delitos

[5]ERTZAINTZA:«Prevención frente a la delincuencia informática» [en línea] [consultado el 11 de marzo de 2012] Disponible en: http://www.ertzaintza.net/public/wps/portal/ertzaintza/

empiezan a afectar la identidad y la vida privada. Los ladrones utilizarán la información de varias maneras, incluyendo el acceso a cuentas bancarias, la creación de tarjetas de crédito u otros fraudes financieros. A veces, van más allá amenazando y molestando a las víctimas. La última ola es el establecimiento de una industria criminal global, cometida por pandillas (grupo de personas) de forma organizada, utilizando métodos bien establecidos. Cobran casi medio mil millones de dólares cada año.[6]

3. Tipos de delitos informáticos

Tomando en consideración los objetivos requeridos, los delitos informáticos se dividen en tres clases: delitos con fines políticos, delitos con fines económicos y otros con fines sociales. Nos limitamos aquí a dar ejemplos sobre los dos últimos puesto que tienen relación directa con nuestro trabajo. Merece la pena recordar que nuestra encuesta va dirigida a estudiantes que utilizan las diferentes redes sociales y que pueden ser afectados por tales tipos de delitos.

3.1. Delitos con fines económicos

3.1.1. Phishing

Se denomina también "suplantación de identidad", es un tipo de robo de identidad en el que el delincuente conocido como Fisher usa mensajes engañosos que no se diferencian mucho de los reales con el fin de orientar a sus víctimas hacia correos o sitios falsificados.Se les pide luego, por motivos de seguridad, introducir informaciones personales como nombre de usuario, contraseña, datos bancarios, etc. La disponibilidad de estos datos hace más fácil el fraude.

3.1.2.Pharming

Este tipo va más allá del Phishing, de modoque el delincuente utiliza unos sitios web muy parecidos a los reales para que el víctima acceda e introduzca su nombre y sus datos personales y no se limita a enviar mensajes de sitios ya existentes.Dicho de otra manera, tal como explica la Agencia Española de Protección de Datos (AEPD),Pharminges el método utilizado para realizar ataques de «phishing» con el objetivo de engañar a los usuarios,

[6]RINALDE Paola (2000) «¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético», disponible en https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

invadiendo sus datos privados y, particularmente, los datos bancarios.La víctima se da cuenta del engaño muy tarde cuando nota un movimiento extraño de dinero en sus cuentas bancarias.

2.1.3. Keylogging

Es un tipo de spyware (espionaje) en el que se usa lo que se llama keylogger que se trata de un virus informático cuya función es registrar y grabar todo lo que escribe la víctima en su teclado con el fin de robar sus informaciones personales como por ejemplo una dirección, una contraseña, posición bancaria, etc.

3.1.4. Sniffing

Es una técnica delictiva de escuchar y captar todas las informaciones circulantes por una red Wi-Fi pública no protegida ni cifrada en el que los hackers roban datos personales como contraseñas y números de tarjetas de crédito, utilizan aquí herramientas informáticas especiales.

3.1.5. Ciberextorsión

Consiste en hackear los correos electrónicos o las redes sociales de una persona, robando informaciones y registrando actividades privadas. El delincuente, en este caso, pide un cierto pago a cambio de no publicar los datos requeridos que pueden ser fotos, documentos, videos y deja un mensaje a la víctima que contiene la dirección electrónica e información donde debe opositar el dinero para que se le muestre una herramienta que sirve para poder recuperar los datos.

3.2. Con fines sociales:

3.2.1. Ciberbullying:

Literalmente, este término inglés se compone del radical “bullying" que significa acoso o intimidación y el prefijo"ciber" qué refiere al uso de los medios digitales. Se refiere a un tipo de delito, cometido generalmente en el entorno escolar, en el que un menor, o un grupo de menores, molesta, amenaza, hostiga intencionalmente a otro menorde forma agresiva y repetida. Según el Estudio sobre hábitos seguros en el uso de las TIC por los menores, publicado por INTECO en marzo de 2009, el cyberbulling se define como acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños.

Entre estas actuaciones es cuando se expone en línea informaciones personales de alguien sin su consentimiento, lo que se conoce por “Doxing” o colarse en las redes sociales de alguien y realizar publicaciones falsas en su nombre, lo que se conoce por “Fraping”.

Estos gestos pueden sobrepasar su limitado espacio electrónico y desviarse a enfrentamientos físicos entre la víctima y el delincuente.

Este mismo delito se puede realizar entre adultos, pero lleva como nombre "**Cyberstalking".**En este caso, está involucrado el tema sexual generalmente.

3.2.3. Grooming

Se trata de un conjunto de conductas y acciones emprendidas por un adulto con el objetivo de establecer una relación con un menor y ganarsu conciencia. Como consecuencia, el adolescente intercambia imágenes y realiza vídeos chats privados con el delincuente y eso conduce a un abuso sexual en el que el niño será obligado a obedecer para que sus imágenes no se publiquen.

3.2.4. Sexting

Es el envío de contenidos eróticos y pornográficos por medio de las redes sociales, el material empieza a difundirsecuando se pierde el control sobre él.

3.2.5. Sextorsion

Se llama también "chantaje", es un delito informático en el cual una persona es chantajeada con una imagen o un vídeo inadecuados (en que aparece desnuda por ejemplo) que han sido compartidos previamente mediante el sexting. El delincuente pide cambios maliciosos y amenaza la victima divulgar estos contenidos si no obedece.

3.2.6. Difamación y calumnia

Este tipo toca tanto a personas como a empresas. En este caso, el delincuente exagera bajo la denominada"libertad de expresión", publicando comentarios y noticias que pueden ser sólo mentiras con el fin de dañar el honor y la reputación de dicha persona o empresa.

En seguida, citaremos algunos casos concretos de los grandes ataques cibernéticos cometidos a nivel mundial:[7]

- **1999**– Se lanza el virus Melissa. Se convierte en la infección informática más agresiva hasta la fecha y resulta ser una de las primeras convicciones para alguien que escribe malware. El virus Melissa era un macro-virus con la intención de apoderarse de cuentas de correos electrónicos y enviar correos masivos. El escritor del virus fue acusado de causar más de 80 millones de dólares en daños a las redes informáticas y fue condenado a cinco años de prisión.

[7]RINALDE Paola: «¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético», disponible en https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

- **2000** –El minorista de música CD Universe es extorsionado por millones después de que la información de tarjetas de crédito de sus clientes fuera publicada en línea. Se lanzan los ataques de Denegación de Servicio (DDoS) contra AOL, Yahoo! Ebay y muchos otros, en varias ocasiones. Las noticias falsas causan que las acciones de Emulex caigan casi un 50%. El virus I Love You se propaga a través de internet.
- **2002** – Se lanza el sitio web Shadow Crew, era un tablero de mensajes y un foro para hackers de sombrero negro. Los miembros podían publicar, compartir y aprender a cometer una gran cantidad de delitos cibernéticos y evitar la captura. El sitio duró dos años antes de ser cerrado por el Servicio Secreto. 28 personas fueron detenidas en Estados Unidos y otros 6 países.
- **2003** – SQL Slammer se convierte en el gusano de propagación más rápido de la historia. Infectó servidores SQL y creó un ataque de denegación de servicio que afectó las velocidades a través de internet durante bastante tiempo, se extendió a través de casi 75.000 máquinas en menos de 10 minutos.
- **2007** – Los casos de hackeo, robo de datos e infecciones de malware se disparan. El número de registros robados y máquinas infectadas aumentan en millones, la cantidad de daños causados en miles de millones.

Recapitulamos diciendo que el delito informático no es un fenómeno reciente ya que existía antes de la aparición de internet y causó grandes problemas tanto a los gobiernos como a los individuos. Internet y las redes sociales proporcionan a los hackers un refugio cómodo para practicar delitos informáticos de forma profesional, organizada y oscura, debido a la vulnerabilidad y la facilidad de acceso a cualquier sitio en cualquier tiempo y lugar, eliminando así todo tipo de barreras espaciales y temporales.

4. Características del delito informático

Los delitos informáticos constituyen uno de los problemas más graves de que padece la sociedad actual ya que ofrecen un sinfín de facilidades a la hora de su comisión y se caracterizan por una serie de particularidades específicasque los hacen distinguirse de los delitos en general. La complejidad principal de este fenómenoconsiste en la dificultad de comprobar y, por lo tanto, de perseguir quien lo comete debido a la gran expansión de la red digital y al carácter técnico de estos hechos.

En seguida, explicaremos las características más decisivas e influyentes de este fenómeno:

- La permanencia y la reiteración:

Los delitos informáticos se pueden repetir de manera continua, tal como señala Rovira Del Canto «*la incidencia de la posible repetición de una actuación ilícita en el ámbito informático favorece su nueva comisión, incluso en múltiples ocasiones*»[8]. Por otra parte,las pérdidasque producen estas acciones pueden ser permanentes o bien difíciles de recuperar.Se refiere aquí, en particular, a los delitos técnicos cometidos por expertos en informática y en programación de sistemas como aquellos que afectan empresas gubernamentales oadministraciones privadas como bancos por ejemplo, causando el mal funcionamiento de sus sistemas y sus dispositivos informáticos, pérdidas de documentos, archivos y pérdidas financieras considerables. Paola Rinaldi trata de los delitos cometidos por pandillas organizadas:

> Según estimaciones de expertos en seguridad cibernética de las Naciones Unidas, aproximadamente el 80% de todos los delitos cibernéticos está siendo cometido por pandillas sofisticadas de criminales que participan en operaciones altamente organizadas. Las pandillas operaban igual que las empresas legítimas, ya que mantenían horas laborales regulares con una jerarquía de miembros, trabajando en conjunto para crear, operar y mantener cualquier fraude en el que se centraban.[9]

Al lado de estos delitos técnicos, existen otros muy simplesllevados a cabo por delincuentes no especializados con la ayuda de algún soporte como por ejemplo los manuales que explicanlos procedimientos de phishingo de keylogger u otros tipos de delitos tratados en apartados anteriores.

- La globalización y el traspaso de las fronteras espacio-temporales:

En efecto, la aparición de Internet que permite la conexión desde cualquier lugar del mundo, hace que los delitos informáticos no se limiten a puestos locales, sino sobrepasan las

[8]ROVIRA DEL CANTO, Enrique (2000): Delincuencia *informática y fraudes informáticos*, Granada, Editorial Comares, p. 78.

[9]RINALDE Paola: «¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético», disponible en https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

fronteras geográficas, suprimiendo así las barreras espaciales, de modo que no importa estar presente físicamente en el lugar donde se comete el delito.En este sentido, Rovira de Canto nos explica:

> La transnacionalidad de los delitos informáticos trascienden las fronteras de los Estados, lo que hace recomendable regulaciones también transnacionales de este tipo de actividades criminales. La transnacionalidad es un tema preocupante ya que un delincuente japonés puede cometer una estafa en Estados Unidos, estando físicamente en Francia, a través de una red de ordenadores controlados 98 remotamente localizados en Rusia.[10]

Por otro lado, y eso es aún más grave, puede no haber coincidencia entre el momento de utilizar el ordenador o el dispositivo y el momento de realizar el delito, por ejemplo se puede enviar un virus hoy mientras que el daño o el hacking se producirá días o semanas después.

- Dificultad de descubrirse

Además de la distancia física y temporal del crimen tratada en el punto anterior, el ciberdelincuente utiliza softwares de última generación y técnicas de redes para enmascarar sus actuaciones y borrar sus huellas en la mayoría de los casos, lo que hace difícil descubrirlo y perseguirle jurídicamente.

5. Delitos informáticos en Argelia

Argelia se clasifica con los países que han evolucionado notablemente en la integración de la tecnología digital en la vida económica y social, es considerada uno de los países en los que el porcentaje del uso de Internet va creciendo constantemente. Pero por otra parte, está en la cima de los países árabes en el campo de la ciberdelincuencia, ha sido en los últimos años testigo de un montón de ciberdelitos electrónicos que provocan desgracias sociales y pérdidas financieras. En efecto, y según las estadísticas presentadas por la gendarmería y la policía nacionales,se registra cerca de 2.500 casos de delitos electrónicos durante el año 2017 entre piratería, extorsión, difamación, acoso y fraudes.El 80% de los delitos cometidos,según el servicio de seguridad encargado de combatir el delito cibernético,

[10]ROVIRA DEL CANTO,Enrique, op. cit., p 78.

fueron a través de la red social "Facebook", de modo quevarias personas han sido víctimas de chantajes y amenazas de publicar sus datos personales.

La mayor parte de las víctimas amenazadas con publicar sus fotos o videos no se atrevan denunciar ni perseguir al delincuente, prefieren sufrir en silencio para proteger su honor y su reputación. La socióloga argelina Zahra Kassi, en una entrevista con el canal televisivoDW árabe, señala que en la sociedad argelina muchas mujeres argelinas acabaron por rendirse anteel chantaje y entregaron grandes sumas de dinero a los delincuentes a cambio de no publicar sus fotos. Otras escapan y abandonan sus familias y maridos temiendo el escándalo. La socióloga insiste al final de su conversación sobre la necesidad de «*difundir la cultura de denunciar al delincuente en la sociedad argelina y percibir el servicio de seguridad nacional como un dispositivo auxiliar y no un medio para reprimir al ciudadano*»[11]

El canal entrevea con dos casos concretos afectados por este fenómeno en Argelia: la primera es Laila Belkacem, profesora titular de historia en la universidad de Relizane y la segunda se trata de una abogada de 26 años llamada B. Samah.

La profesora Belkacem narra este capítulotrágico de su vida: «Mi vida se convierte en un infierno por culpa de una persona que no conozco ni en el mundo real ni en el virtual. Me acusó de varias cosas, incluyendo pertenecer al Rotary Club y a los masones. Las publicaciones diarias comenzaron a acusarme hasta tocar mi honor y mi ética, me califican de lesbiana y de tener relación con tal y tal. Otras acusaciones tenían como objetivo chantajear y golpear mi reputación, incluidas las actividades intelectuales que comencé desde 2015».[12]

La profesora sigue diciendo que la situación se empeoraba aún más cuando sus estudiantes y sus colegas se dieron cuenta de estos rumores, lo que influye negativamente sobre su relación con ellos.

La profesora acude a la justicia, pero el delincuente sigue siendo libre y continúacometiendo crímenes a través de sus páginas hasta ahora, algo que le enfada mucho.

En cuanto a la abogada "B Samah", recibió un mensaje a través de Facebook de un pirata informático, le amenazó con publicar fotos de su matrimonio,celebrado dos meses antes, en caso de que no le enviara una suma de dinero en su cuenta de correo que definirá más tarde.El hacker envió otro mensaje pidiendo dinero sin especificar la cantidad. Lo que

[11]«Ciberdelincuencia en Argelia: el "escándalo" como el arma más poderosa de los perpetradores» (2018), الجريمة الإلكترونية بالجزائر- "الفضيحة" أعتى أسلحة الجناة(artículo original) en https://www.dw.com/ar%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9 42522945.

[12] Ibid.

lleva a la abogada y su esposo decidir ir a la policía. Afortunadamente, la policía logró identificar a los dos delincuentes: un adolescente y un adulto.

La historia de la profesora Layla y la abogada Samah, no es más que una gota en un mar contaminado por las historias de chicas y chicos que han sido víctimas de delincuentes en el mundo virtual. Argelia sigue siendo en la cabeza de la lista de los países que padecen de los delitos informáticos, por este motivo las autoridades tienen que poner fin o disminuir a estos vicios que afectan a nuestra sociedad y revisar urgentemente las leyes relacionadas con los crímenes digitales.

6. Consejos para evitar los delitos informáticos

Las redes sociales representan uno de los lugares favoritos de los ciberdelincuentes puesto que estas plataformas contienen una gran cantidad de datos e informaciones personales de los usuarios bajo formas diferentes: imagen, videos, textos y documentos escritos, etc. Por estas razones, la seguridad a la hora de conectarse y consultar estasredes debe ser una cuestión que preocupa cada navegante puesto que en el otro lado existe un grupo de personas cuyo tiempo se dedica solamente a hacer actividades fraudulentos y molestar a la gente, apropiándose de su identidad y utilizarla para fines inhumanos.

A continuación, sugerimos algunas recomendaciones que nos protegen a la hora de navegar y utilizar las redes sociales y reducen el riesgo de caer a manos de los criminales y ser uno de sus víctimas:

- Rechazar mensajes no adecuados y solicitudes por parte de desconocidos.
- Evitar publicar fotos personales en redes públicas para evitar su utilización ilícitamente
- Utilizar perfiles privados y limitar las personas que pueden ver tu perfil y tus publicaciones para que el contenido sólo sea accesible a familiares o amigos, se debe configurar la opción “cuenta privada” en la ventana “opciones”, con el fin de evitar que extraños observen las fotografías y comentarios del usuario.
- Leer bien la política de privacidad que proponen los diferentes sitios consultados antes de crear cuentas y diseñar perfiles.
- Utilizar siempre un antivirus en las computadoras personales.
- Es mejor utilizar contraseñas privadas y complejas y cambiarlas frecuentemente(Debe ser una contraseña única que contenga como mínimo 13 caracteres, entre los cuales deben incluirse letras, símbolos y números.)

- No aceptar los mensajes de tipo sexual o pornográfico
- Navegar por páginas seguras(deben empezar por http://).
- No se aconseja colocar el nombre del usuario, la fecha de nacimiento o el número de carnet de identidad porque son los primeros datos que utilizan los hackers.
- Cuando se sospecha de la privacidad de la cuenta, se debe cambiar la contraseña de inmediato y revisar ajustes.
- Desactivar el geo localizador: es primordial desactivar el sistema GPS porque permite descubrirel lugar donde se encuentra el usuario al rastrear su Smartphone.Esto es especialmente arriesgado cuando la persona está de viaje o fuera de casa ya que los delincuentes podrían acceder a la propiedad.

Dentro de este contexto, Rinalde Paola[13]dice queno hay garantía de que no serás hackeado, pero puedes limitar seriamente los riesgos. Para conseguir eso nos propone utilizar una herramienta denominada VPN (la Red Privada Virtual). Su función consiste en crear conexiones seguras que son indetectables y no rastreables, utilizando una técnica de protección basada en el cifrado o la codificación de los datos:

> Se puede utilizar para proteger dispositivos individuales o toda una red. Se puede utilizar para proteger a tu familia o negocio de ataques externos, o para conectar un dispositivo remoto a una red doméstica con seguridad. La mejor parte es su cifrado, la tecnología que codifica tus datos en jibberish ilegible, debido a que hace que atacar al usuario de una VPN sea tan difícil y consume tanto tiempo que los sombreros negros son más propensos a buscar presas más fáciles, en lugar de perder su valioso tiempo en ti.[14]

Conclusión

Al final de este capítulo, se puede decir que cualquier error al utilizar las redes sociales da la oportunidad a miles de delincuentes que pasan mucho tiempo delante del

[13] Paola Rinaldi es una traductora, transcriptora y escritora freelance que colabora con Le VPN desde julio de 2015, administrando las redes sociales. Como escritora del blog de Le VPN en español escribe artículos de interés y noticias actuales acerca de todo lo relacionado con la seguridad y privacidad en internet, el entretenimiento y la protección de datos personales.

[14] RINALDE Paola: «¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético», disponible en https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

ordenador, esperando un probable descuido por parte de losusuarios para robar sus datos personales y utilizarla ilegalmente por beneficios suyos.Esto afecta la vida de la víctima tanto económica a través del robo de números de tarjetas de créditos o social a través de chantajes que tocansu honor y su reputación. Para evitar, o a lo menos, reducir los riesgos de estos delitos, es necesario seguir algún protocolo de protección y tener conocimiento sobre políticas y métodos de privacidad que nos mantienen en estado seguro a la hora de conectarnos.

Capítulo n° 3

Análisis de los datos e interpretación de los resultados

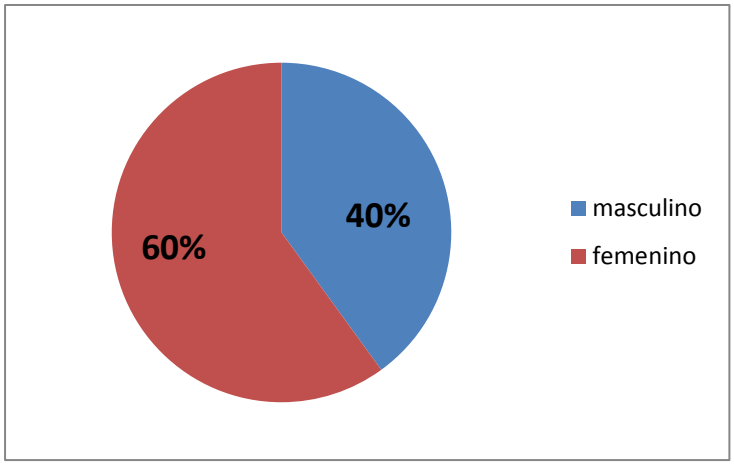
1. Metodología de trabajo

Nos contamos con una metodología de investigación basada sobre la muestra que consiste en una encuesta[1]sobre las redes sociales y la ciberdelincuencia que puede generar el mal uso de las mismas. En paralelo,analizamos las respuestas de los encuestados. El objetivo deseado es saber qué popularidad han obtenido estas plataformas digitales entre los jóvenes de hoy, y particularmente, en nuestro entorno universitario y si los internautas están conscientes de los denominados delitosinformáticos y la gravedad de los efectos perjudiciales que producen. Por otra parte, pretendemos medir hasta qué punto están preparados para enfrentar este fenómeno, a través de adoptar algunas conductas que permiten protegerlos a la hora de navegar.

2. La muestra

La tabla n°1 indica la muestra de nuestra investigacióny que contiene veinte encuestados: 8 de género masculino y 12 de génerofemenino, todos son estudiantes del departamento de la lengua española de la universidad de Abdelhamid Ibn Badis, Mostaganem. Su edad es entre 19 y 24 años.

Género	Número de personas	Porcentaje
Masculino	8	40%
Femenino	12	60%



[1] Véase el anexo 1.

Laspreguntas que hemos dirigidoa los veinte encuestados constan de 16 preguntas, algunas son directas (cerradas) cuya respuesta necesita la confirmación o la negación del contenido, mientras que otras preguntas exigen elegir una o varias opciones propuestas previamente.

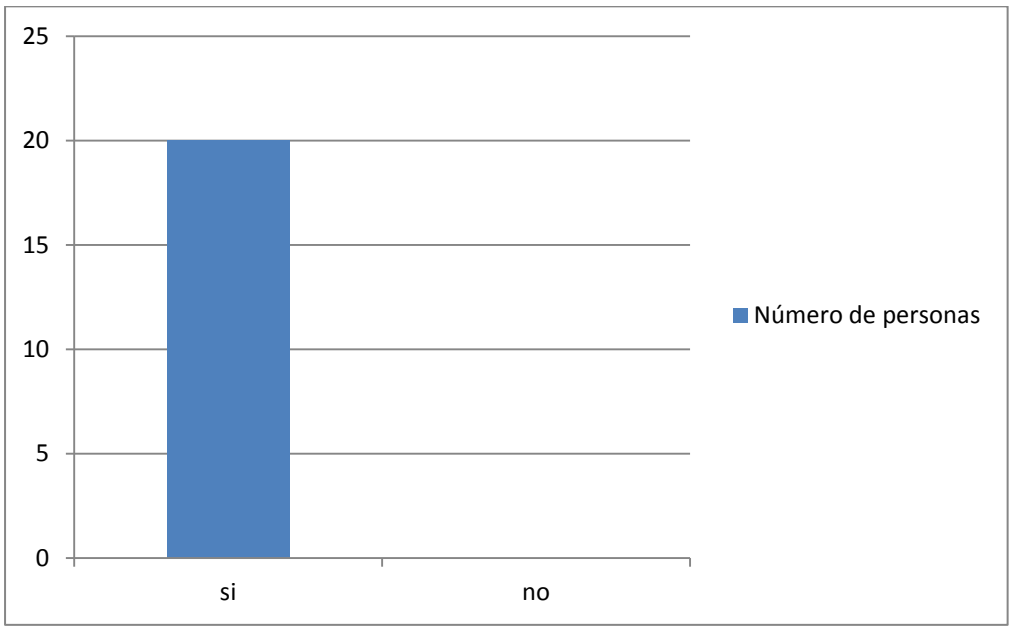
2. Análisis del corpus

A continuación, pasamos a exponer los datos recolectados y analizarlos, siguiendo el mismo orden en que aparecen las preguntas en el cuestionario:

Pregunta n°1: ¿Eres un usuario de las redes sociales?

Los siguientes tabla y grafico muestran las personas que utilizan las redes sociales:

	Número de personas	porcentaje
si	20	100%
no	0	0%



Comentario

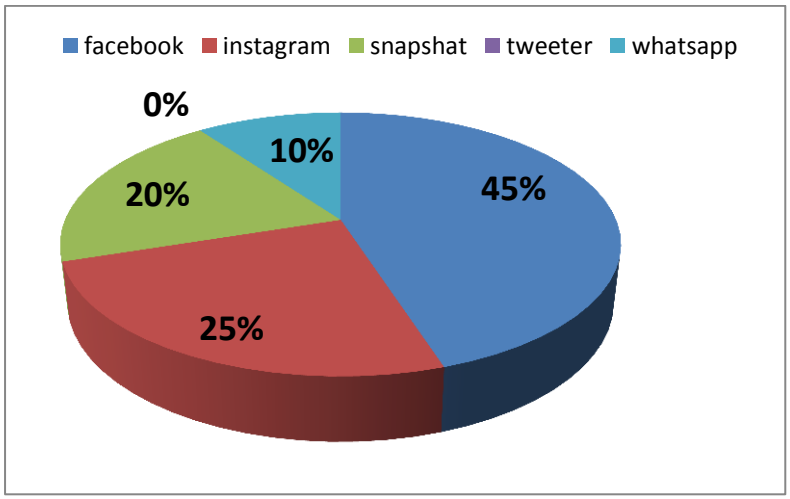
En efecto, las respuestas han sido sorprendentesa medida que el 100% hanrespondido por sí, confirmadoasí su utilización de las redes,es decir que casi todos los estudiantes forman parte de estas plataformas hoy en día,lo que muestra su importancia en la vida de los mismos.

Lo llamativo también es la coincidencia de estos datos con las estadísticas que se hacen anualmente sobre el grado de integración de las tecnologías digitales en la vida de los argelinos, de modo que el porcentaje crece constantementeaño tras otro.

Pregunta n° 2: ¿Qué son las redes que más utilizas?

La tabla y el gráfico siguientes demuestranla red social más usada por los encuestados.

Redes sociales	Número de personas	Porcentaje
Facebook	9	45%
Instagram	5	25%
Snapshat	4	20%
Tweeter	0	0%
Whatsapp	2	10%



Comentario

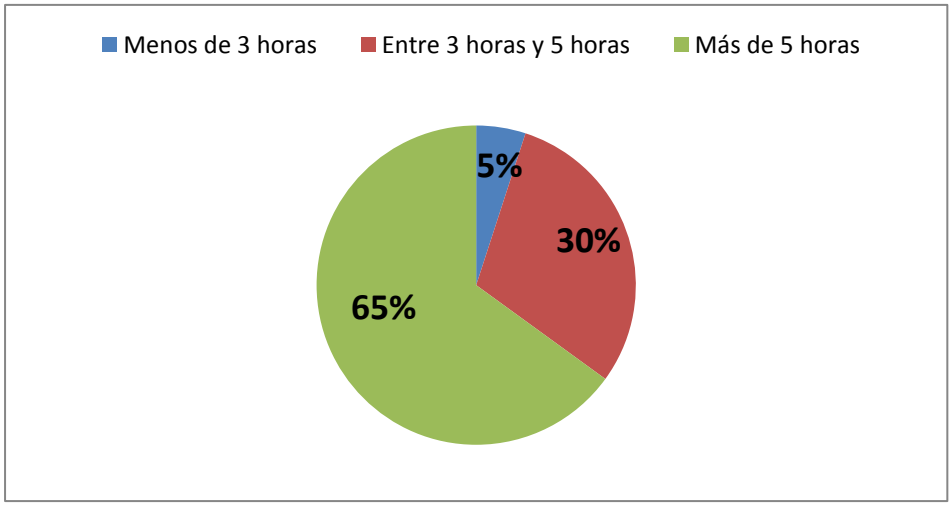
Partiendo de los resultados recogidos, notamos que Facebook es la red más utilizada entre los estudiantes.En nuestra opinión, esto es evidente y lógico puestos que se considera como la red más antigua y más famosa a nivel mundial y no solamente en nuestro entorno universitario. Por otra parte, si nos referimos a la historia de Facebook, tratada en el primer capítulo, encontramos que la creación de esta red el año 2004 por parte de Mark Zuckerberg junto con sus compañeros tenía como objetivo poner en contacto a los estudiantes de la

universidad de Harvard para compartir resúmenes, noticias y trabajos. Luego, con el paso del tiempo y la traducción de sus páginas a muchas lenguas ganará la popularidad que tiene hoy entre las diferentes categorías sociales.Después de Facebook llega instagram y snapshat que son casi similares en cuanto al uso ya que hoy en día estas dos plataformas se utilizan frecuentemente,especialmentepor parte de las chicas que la prefieren másen comparación con los chicos. Despuésviene whatsapp que es una plataforma de mensajeríainstantánea y, por fin, tweeter que no atrae a ninguno de los cuestionados, esta plataforma es más profesional y se usamás por los famosos para publicar comentarios cortos y expresivos para interactuar con sus fans.

Pregunta n° 3: ¿Con qué frecuencia usas esta red por el día?

La tabla y el gráfico abajo muestran la frecuencia del uso de las redes sociales por el día por parte de nuestros encuestados.

	Número de personas	porcentaje
Menos de 3 horas	1	5%
Entre 3 horas y 5 horas	6	30%
Más de 5 horas	13	65%



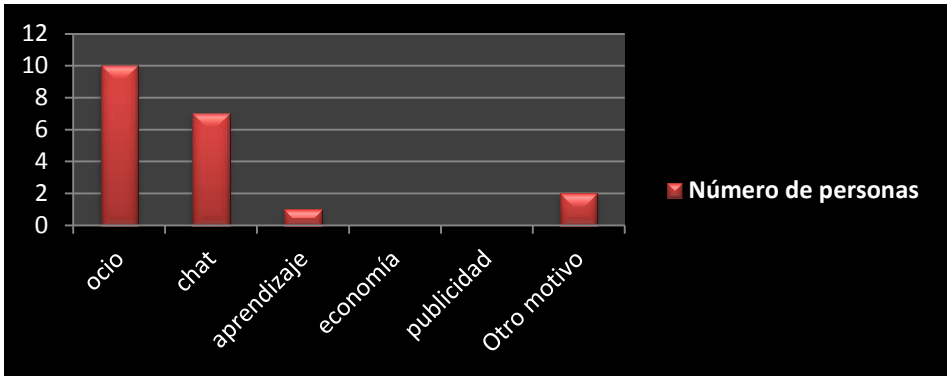
Comentario

Notamos que la mayoría de los encuestados,representados por el 65%, utilizan estas plataformas digitales más de cinco horas por el día, un tiempo que es duradero y muy largo, lo que significa, para nosotros, que son adictos y no pueden imaginar a sí mismos desconectados de este mundo digital.Por otra parte, eso indica que Internet se incorpora notablemente en la vida diaria de los estudiantes, convirtiéndose en un elemento indispensable.

Pregunta n°4: ¿Para qué utilizas esta red?

En los siguientes tabla y gráfico cabe mencionar el motivo del uso de las redes sociales por parte de nuestros cuestionados.

	Número de personas	porcentaje
Ocio	10	50%
Chat	7	35%
Aprendizaje	1	5%
Economía	0	0%
Publicidad	0	0%
Otro motivo	2	10%



Comentario

Notamos que la mitad de los estudiantes utilizan estas plataformas digitales para un solo motivo que es el ocio y el 35% las usan para chatear con amigos, familia etc., mientras que son pocos los que tienen como objetivo el aprendizaje. En cuanto a la economía y la publicidad se ve que nadie utiliza las redes para estos dos motivos (0%).

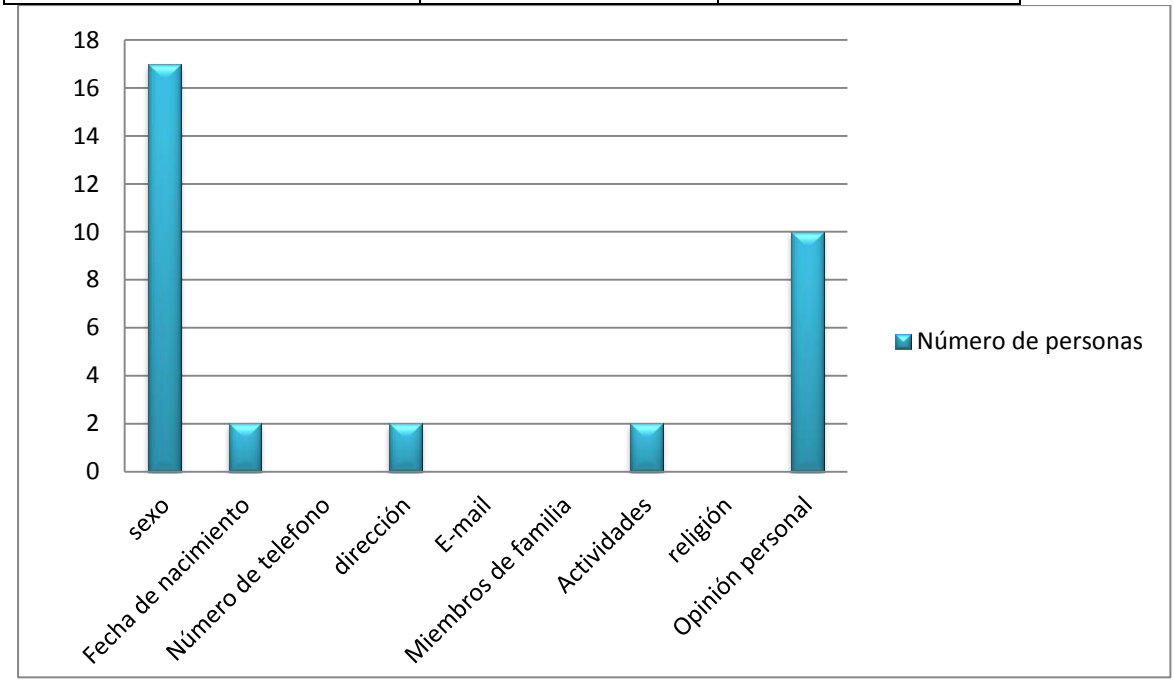
Tomando en consideración estos datos, se puede decir que la mayoría de los estudiantes acuden a las redes para chatearcon amigos y familiares o gente nueva y compartir con ellos informaciones, experiencias privadas, eventos y sentimientos, mientras que no aprovechan de los beneficios que permiten estos espacios en los dominios económicos e intelectuales. Tal vez prefieran otras opciones para su investigación científica y para su futura vida laboral (y sobre todo en lo que concierne la búsqueda de puestos de trabajo). Por otra parte, hay que reconocer la importancia de estas redes como medio de comunicación entre los estudiantes de cada promoción entre sí y entre ellos y sus profesores. En efecto, estos últimos transmiten muchas noticias por medio de los delegados a toda la promoción, ganando así tiempo y esfuerzo y sobre todo en los períodos en que hay algunas circunstancias como es el caso del Harak, huelgas o la epidemia de Covid 19 que actualmente paraliza todo el país. Esto permite también a otros estudiantes que no pueden asistir por culpa del trabajo estar al corriente de todas las novedades sin desplazarse.

Pregunta n° 5: ¿Qué información sueles exponer en tu perfil? (varias opciones)

La tabla y el gráfico siguientes describen la naturaleza de las informaciones que suelen exponer nuestrosencuestados en sus perfiles.

	Número de personas	Porcentaje
Sexo	17	52%
Fecha de nacimiento	2	6%
Número de teléfono	0	0%
Dirección	2	6%
E-mail	0	0%
Miembros de familia	0	0%

Actividades	2	6%
Religión	0	0%
Opinión personal	10	30%



Comentario

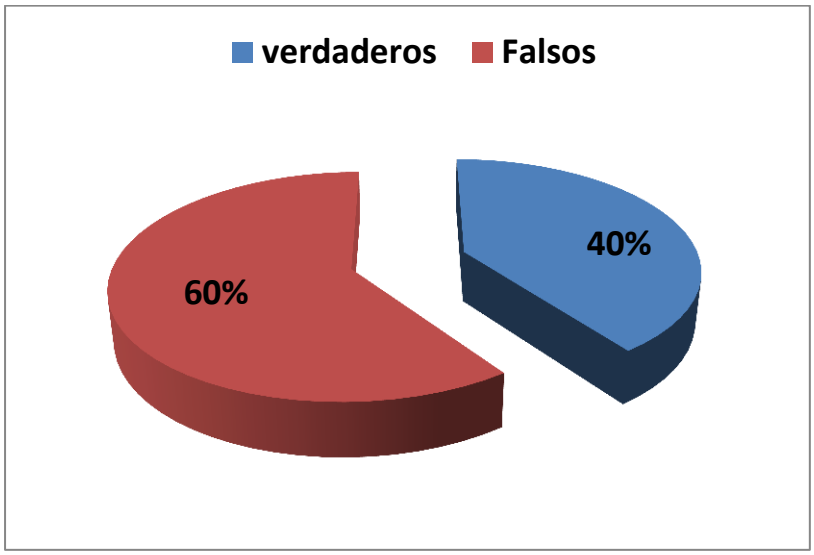
Como se muestran bien en las estadísticasexpuestas, nadie agrega su número de teléfono ni los miembros de su familia,tampoco su E-mail, lo mismo por la religión. Sólo mencionan datos neutros como el género o la edad o expresan una opinión personal que refleja su pensamiento para llamar la atención.

Esto se puede explicar por la voluntad de estos estudiantes, de sexo femenino sobre todo, de esconder su propia identidad para que no sean descubiertos en estas plataformas o bien no ponen confianzaen las mismas. Este comportamiento se puede explicar también desde un punto de vista sociológico, de modo que la mayoría de los hombres argelinos no aceptan que el mundo femenino de su familia (hermanas, hijas y esposas) sea accesible por extranjeros.

Pregunta n°6: Los datos personales que proporcionas en tu perfil sonverdaderos o falsos:

Véase la tabla y el grafico siguientes.

	Número de personas	Porcentaje
verdaderos	8	40%
Falsos	12	60%

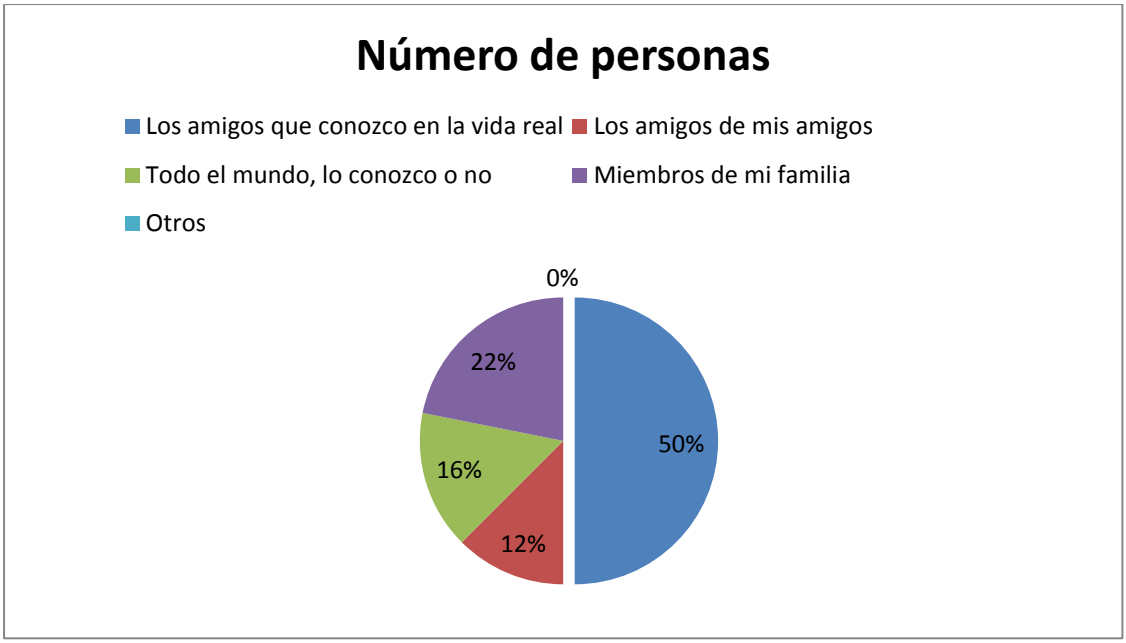


Comentario

Se nota queel 60% de los estudiantes poneinformaciones falsas en sus perfiles (la mayoría de ellos son chicas). Lo que se puede explicar otra vez por su voluntad de disimular su verdadera identidad, o sea por razones personales y sociales o bien temiendo de las malas intenciones de los llamadosciberdelincuentes.

Pregunta n° 7:¿A quién añades a tus listas de amigos? (varias respuestas posibles)

	Número de personas	Porcentaje
Los amigos que conozco en la vida real	16	50%
Los amigos de mis amigos	4	12%
Todo el mundo, lo conozco o no	5	16%
Miembros de mi familia	7	22%
Otros	0	0%

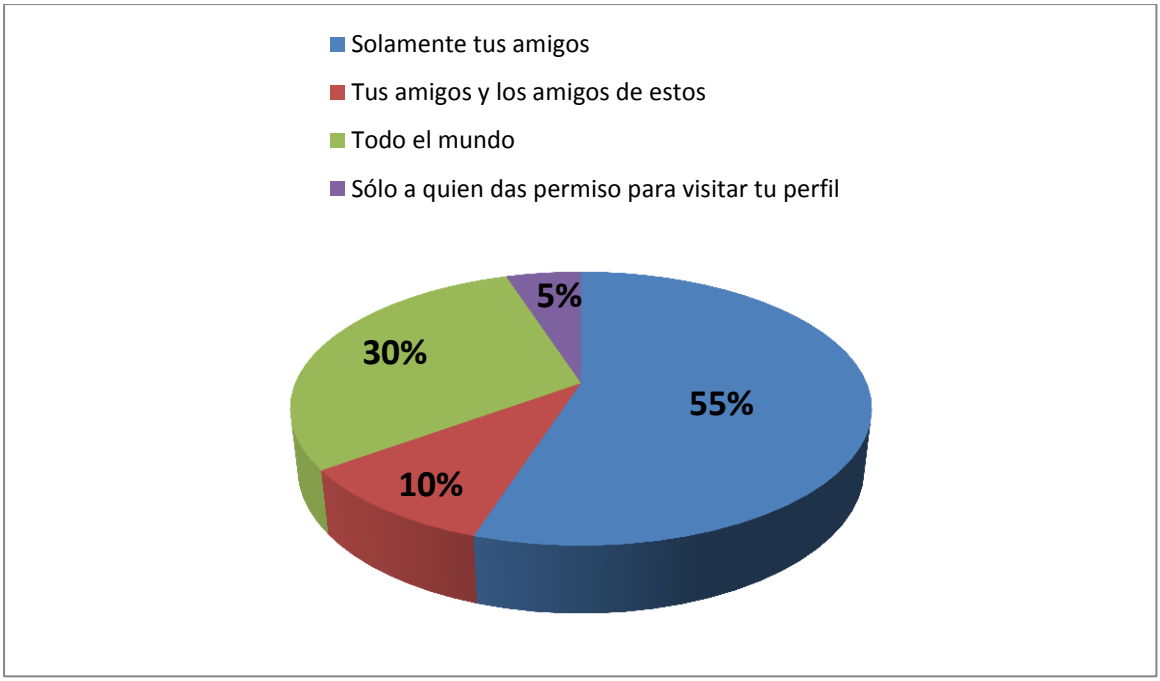


Comentario

Mediante los anteriores gráficoy tabla observamos que la mitad de los encuestados ponen confianza solamente en los amigos que frecuenten en la vida real y el 22%añadenademás sus miembros de familia, sólo el 16% incluyen a los desconocidos y son generalmente los chicos. Esto muestra que los estudiantes están conscientes de los peligros que puede producir el hecho de integrar a sus listas de amigos a gente extranjera y desconocida, toman todas sus precauciones para proteger sus datos personales, lo que explica que están al corriente del fenómeno de los delitos informáticos.

Pregunta n°8: ¿Quién puede consultar tu perfil?

	Número de personas	Porcentaje
Solamente tus amigos	11	55%
Tus amigos y los amigos de estos	2	10%
Todo el mundo	6	30%
Sólo a quien das permiso para visitar tu perfil	1	5%



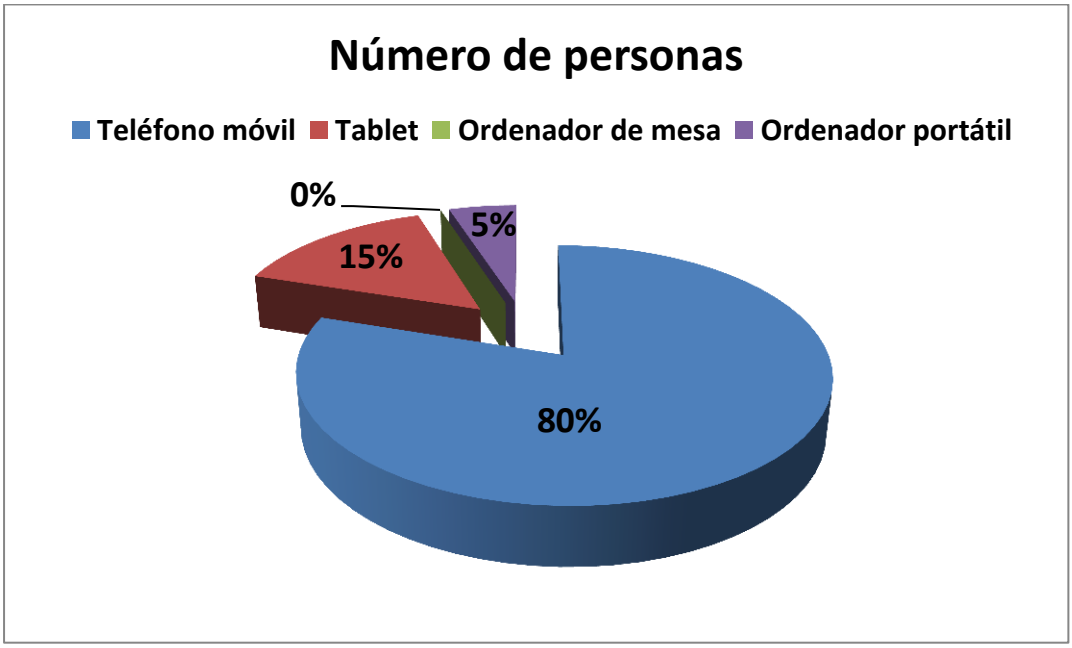
Comentario

Notamos que los estudiantes que permiten sólo a sus amigos ver su perfil sobrepasan la mitad, mientras que aquellos que dejan sus perfiles abiertos a todo el mundo forman el 30%. Solamente el 5% utilizan la opción de permiso. Notamos también que son las chicas que limitan el acceso a sus perfiles a sus amigos y amigas mientras que los chicos dan la oportunidad a todo el mundo. Esto se explica también por razones sociales y familiares, de modo que nuestras tradiciones exigen que el mundo femenino sea más discreto y preservado en su relación con el otro sexo, con los extranjeros. Las chicas, generalmente, toman en consideración su honor y su buena reputación y los de su familia. Por su parte, los padres también insisten sobre este punto y suelen controlar a sus hijas y les comparten la elección de sus compañeros, a veces tanto en el mundo real como en lo virtual. Dentro de este contexto, una prima mía me cuenta que su padre le envía una invitación imprevista por Facebook, lo que le lleva a bloquear inmediatamente toda la lista de amigos y luego toda la cuenta, creando otra nueva. Esta historia puede ser una anécdota pero refleja el contexto social y tradicional en que viven nuestros estudiantes.

Pregunta n°9: ¿Cuáles de las siguientes tecnologías sueles utilizar para conectarte y consultar tus cuentas personales?

Véase la tabla y el grafico siguientes.

	Número de personas	porcentaje
Teléfono móvil	16	80%
Tablet	3	15%
Ordenador de mesa	0	0%
Ordenador portátil	1	5%



Comentario:

A travéslas anteriores tablas y gráfico se ve que el 80% de los encuestados utilizan el teléfonomóvil, mientras que solamente el 20% de ellos usan otros instrumentos para conectarse y nadie utiliza el ordenador de mesa (0%). Esto se explica por las facilidades que permiten los aparatos móviles en comparación con los ordenadores de mesa, de modo que se pueden llevar a cualquier lugar, incluso a la universidad donde nuestros estudiantes pasan la mayoría de su tiempo. Además, actualmente las nuevas tecnologías que permite la comunicación en Argelia, "la cuarta generación/ 4G" facilita la conexión por medio de nuestras propias líneas telefónicas, lo que quiere decir una conexión individual no compartida. Por otra parte, el uso de los móviles se puede explicar desde un punto de vista psicológico, de modo que protege la intimidad de los usuarios al conectarse, pero por otra parte, lleva a su aislamiento del mundo real, de su familia e incluso de sus amigos.

Pregunta n°10: ¿Crees que estás seguro al momento de utilizar la red o uno de estos medios tecnológicos?

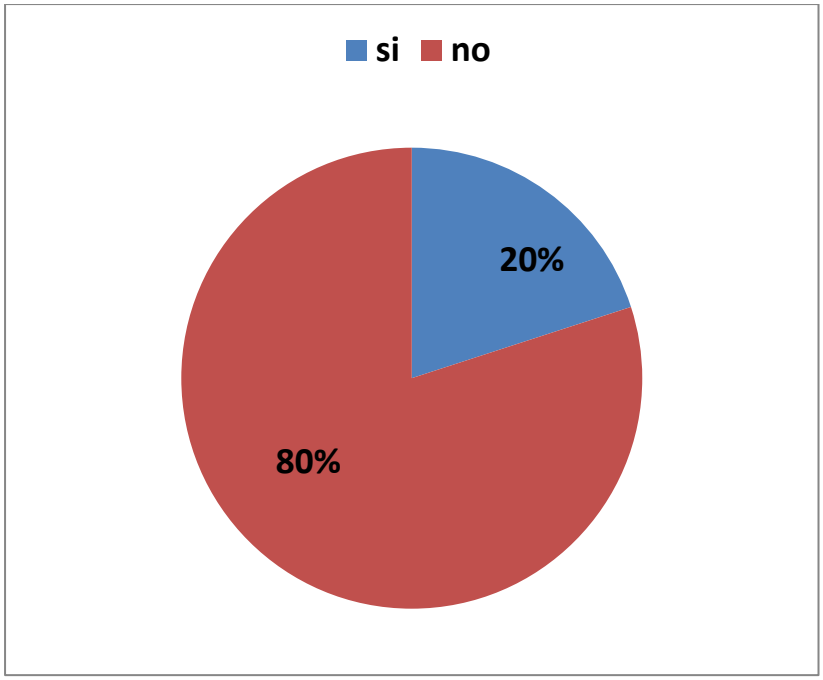
	Número de personas	Porcentaje
sí	8	40%
no	12	60%

Comentario

A partir de estas estadísticas se puede decir que la mayoría de los usuarios de las redes sociales no se sienten seguros en el momento de conectarse, pero, a pesar de eso no dejan de utilizarlas porque son adictos a estas plataformas y no pueden imaginar a sí mismos sin ellas.

Pregunta n° 11: ¿Sueles revisar las opciones de "privacidad" y "seguridad" de las redes sociales antes de crear cuentas y perfiles?

	Número de personas	Porcentaje
si	4	20%
No	16	80%

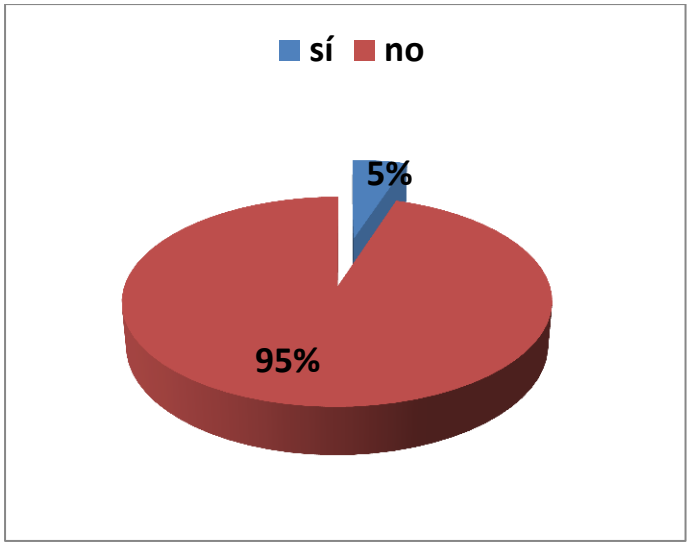


Comentario

Mediante las respuestas se puede decir que la mayoría de los estudiantes no revisan las opciones de privacidad y de seguridad antes de crear sus cuentas. Esto se justifica, a nuestro parecer, por holgazanería y por el aburrimiento que produce la lectura de estos textos que a veces son muy largos. Pero, esto es muy arriesgado porque a veces la política de algunos sitios no corresponde a nuestras voluntades ni a nuestros principios. Los estudiantes deben tener la cultura de leer este tipo de textos por importantes que sean.

Pregunta n°12:¿Conoces algunas técnicas de seguridad informática

	Número de personas	Porcentaje
sí	1	5%
no	19	95%

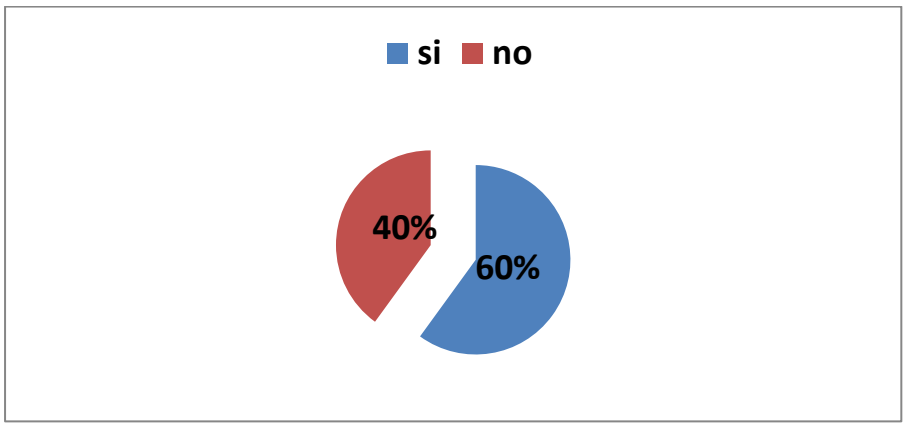


Comentario

A partir de los resultados podemos decir que casi todos los usuarios de las plataformas digitales desconocen las técnicas de seguridad informática.Éstas ayudan para proteger nuestros datos, o a lo menos reducir la posibilidad de ser víctima de un fraude cibernético. No hace falta citar de nuevo estas técnicas tratadas en el segundo capítulo en el apartado titulado "Consejos para evitar los delitos informáticos".

Pregunta n°13: ¿Fuiste alguna vez víctima de un delito informático?

	Número de personas	porcentaje
sí	12	60%
No	8	40%



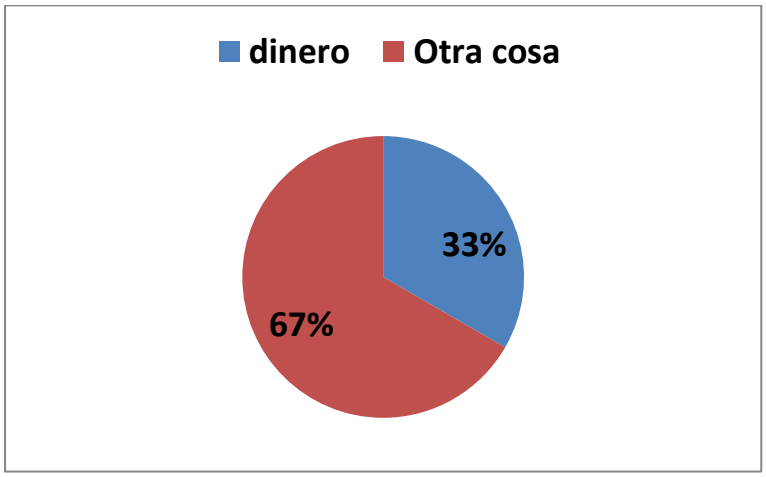
Comentario

Según las estadísticas,notamos que la mayoría de los estudiantes han caído en la trampa de los delitos informáticospor medio de las plataformas digitales.En efecto, este fenómenose convierte en un monstruo que asusta a todos los que utilizan estas plataformas ya que generan muchos problemas tanto económicos como sociales explicados detalladamente en la parte teórica.

Pregunta n°14:¿Qué se te pidió a cambio de tus dispositivos personales?

Esta pregunta va dirigida a los 60% encuestados que han sido una víctimas de un delito informático para saber que se les pide a cambio de sus datos personales robados. Véase la tabla y el grafico siguientes:

	Número de personas	porcentaje
Dinero	4	33%
Otra cosa	8	67%

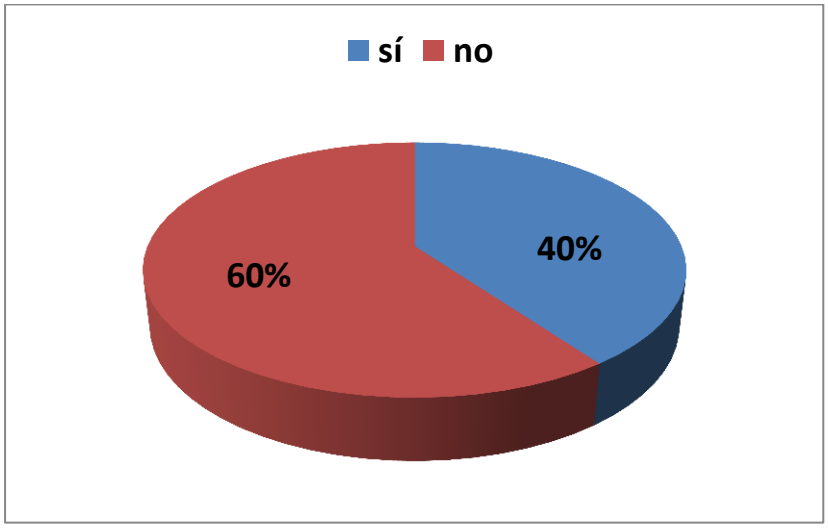


Comentario

El 33% de los 60% de los encuestados que padecen de un delitoinformático; se les pidió dinero a cambio de sus datos personales y el 67% que sobra dicen que los delincuentes solicitaron otras cosas. Estas cosas pueden ser actos inmorales e inhumanosque tocan el honor y la reputación de las víctimas, especialmente las chicas. El delincuente, como ya se ha explicado al tratar de los tipos de los delitos informáticos, acude al chantaje y las amenazas con publicar las fotos y los videos robados.

Pregunta n°15: ¿Sigues poniendo cierta confianza en esta red?

	Número de personas	Porcentaje
Si	8	40%
no	12	60%

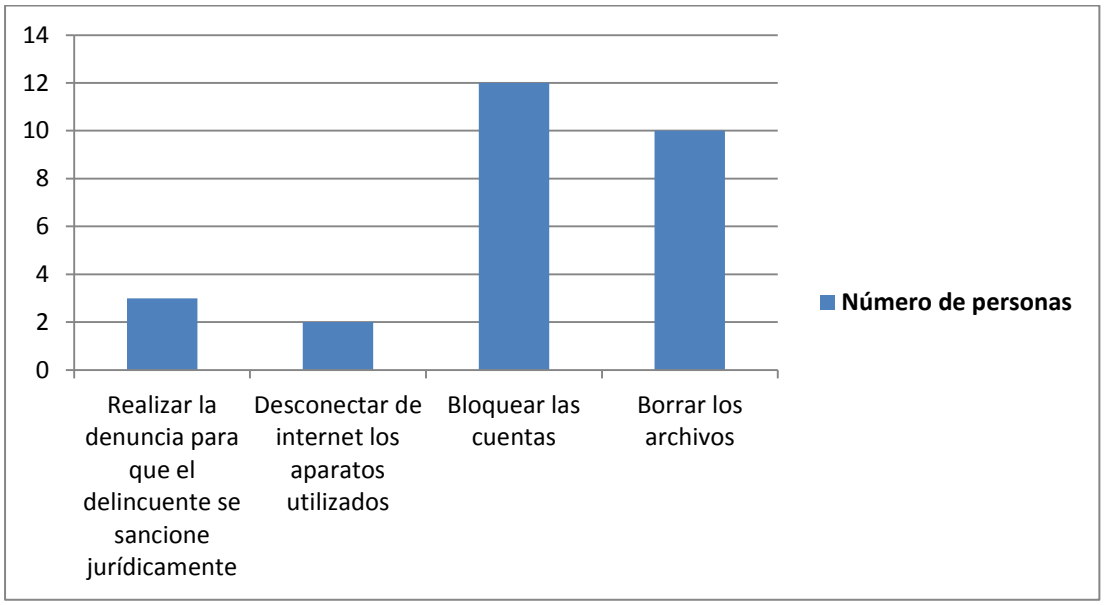


Comentario

Según las opiniones de nuestros encuestados se nota que la mayoría de ellos no pueden confiar más en las redes sociales ya que han enfrentado muchos problemas en su vida diaria por culpa de los fraudes queinvaden su privacidad y su identidad. Pero, por otra parte, como ya se ha señalado antes, no dejan de utilizarlas por adicción.

Pregunta n°16: ¿Cómo tenemos que reaccionar ante un delito informático que afecta nuestra identidad? (varias opciones)

	Número de personas	Porcentaje
Realizar la denuncia para que el delincuente se sancione jurídicamente	3	11%
Desconectar de internet los aparatos utilizados	2	7%
Bloquear las cuentas	12	45%
Borrar los archivos	10	37%



Comentario

A partir de los resultados obtenidos notamos que la mayoríade los estudiantes,víctimas de un delito informático, prefieren bloquear sus cuentas y suprimir los archivos para evitar,más o menos,el contacto con el delincuente y sus molestias. Pero, deben saber que esto no es siempre la solución más adecuada puesto que éste guarda copia de los datos robados. En este caso, es mejor denunciar y acudir a la justicia para perseguir al delincuente y no borrar las huellas del crimen puesto que cada detalle ayuda para detectar la persona que lo comete. Notamos que sólo el 11% han elegido esta solución porque, como ya hemos explicado al tratar de los delitos informáticos en Argelia, los argelinos, y las argelinas sobre todo y según los sociólogos, prefieren no ir a la policía para evitar el escándalo.

Conclusión

Según las respuestas de losestudiantes encuestados, nos constatamos que la mayoría, a pesar de tomar otras precaucionestal como rechazar a los extranjeros por ejemplo, no revisan la política de privacidad que proponen los sitios en el momento de abrir cuentas en las plataformas digitales y desconocen las técnicas de seguridad. Eso puede ser la causa principal, pero no la única, que les lleva a caer a manos de los ciberdelincuentes que están en el otro lado, esperando un probable descuido por parte de los usuarios para invadir su mundo virtual privado, causándoles desgracias en el mundo real público.

Conclusión general

Concluimos diciendo que el presente trabajo es una modesta investigación académica cuyo objetivo es tener una visión global sobre las redes socialesy su incorporación en la vida personal y profesional de los internautas en general y de los estudiantes, en particular. Hemos tratado de los peligros generados por el mal uso de estas plataformas para que estos últimos tomen sus precauciones a la hora de navegar y sepan cómo proteger sus datos personales.

La ciberdelincuencia es un fenómeno muy peligroso, varía entre delitos cuyo fin es la invasión de la identidad de las personas y la agresión de su seguridad y otros que tienen como objetivo dañar sistemas informáticos y electrónicos y espiar información relacionada con empresas e instituciones gubernamentales o privadas:económicas, comerciales o financieras como bancos por ejemplo.

Cuando se trata del primer tipo, que nos interesa aquí, que afecta la identidad de las personas, las pérdidas pueden tenergran impacto sobre la víctima a los niveles económico, social, psicológico y emocional. La posible publicación de las fotos y los videos robados puede generar consecuencias trágicas como por ejemplo poner a dudas la reputación y el honor de la víctima, lo que influye negativamente sobre su relación con los demás, pérdida de empleo, divorcio, complicaciones, etc.

En cuanto a nuestro caso de estudio representado por los estudiantes de nuestro departamento, la muestra que hemos llevado a cabo con ellos indica que casi todosutilizan de forma abusiva y adictiva las redes sociales y no pueden imaginar a sí mismos desconectados de este mundo virtual. Según los datos recogidos, hemos constatado que la mayoría hasido alguna vez víctima de un delito informático. Por otro lado, y lamentablemente, casi todos desconocen las técnicas de seguridad informática que sirven para proteger sus datos, o a lo menos reducir los riesgos del fraude cibernético.

La gravedad de este fenómeno consiste en la imposibilidad de controlarlo ya que sucede todos los días y en todas partes y es difícil de descubrir. Lo único que podemos hacer es estar preparado, comportándose de cierto modo al usar la red y controlar nuestras prácticas de conexión, por ejemplo navegar únicamente por páginas seguras, usar antivirus o antimalware, rechazar mensajes y solicitudes no adecuados por parte de desconocidos y leer bien la política de privacidad que proponen los diferentes sitios consultados antes de crear cuentas y diseñar perfiles.

Por fin, como cada investigación, seguro que nuestro trabajo no llega a ser suficiente para un tema tan amplio como este, por esto esperamos que vaya a abrir puertas para otras investigaciones que estudian más a fondo el tema en cuestión. Dentro de este contexto, y

puesto que notamos que la mayoría de los estudiantes que han sido víctima de un delito informático prefieren no perseguir jurídicamente al delincuente, sugerimos investigar si la ley en nuestro país es efectiva para afrontar el fenómeno del ciberdelito y el daño significativo que lo acompaña a las personas y las instituciones estatales, y qué hace el legislador argelino para adaptar el Código Penal al desarrollo tecnológico en los dominios de la información y de la comunicación.

Fuentes Bibliográficas

Obras completas

CANELO BORJA, Fernández (2010): *Redes sociales: lo que hacen sus hijos en Internet*, San Vicente del Raspeig, Alicante, Editorial Club Universitario.

DAVARA RODRÍGUEZ, Miguel Ángel (1993): *Derecho informático*, Pamplona: Aranzadi.

DARIO CORONEL FIGUEROA, Joel (2015): *Impacto de las redes sociales en los jóvenes y sus consecuencias*, Monografía para la obtención del título de bachiller, Unidad Educativa Santo Domingo de los colorados bachillerato en ciencias.

EROLES, J. L. D. G. (2010) : *Internet Marketing 2. 0: captar y retener clientes en la red*, Barcelona, Reverté.

GALVEZ CLAVIJO, Ismail (2015): Facebook para empresas y emprendedores, Malaga, IC Editorial.

MACÍA, F., y Gosende, J. (2011): *Marketing con redes sociales*, Madrid, Grupo Anaya.

MORENO, Manuel (2000- 2014): El gran libro del Community Manager, Barcelona, Gestión.

MORALES PERÉZ, G. (2011): *Las redes sociales, Conclusiones de un estudio sobre el grado de conocimiento y utilización por profesionales de la formación*, en Ruiz Palmero, J. y Sánchez Rodríguez, J., *Buenas prácticas con TIC para la investigación y la docencia*. Málaga, Universidad de Málaga.

ORIHUELA, José Luis (2011): *Mundo Twitter: Una guía para comprender y dominar la plataforma que cambió la red*, Barcelona, Alienta.

RAMOS, J. (2017). Marketing de contenidos. Guía práctica. XinXii.

ROVIRA DEL CANTO, Enrique (2000): *Delincuencia informática y fraudes informáticos*, Granada, Editorial Comares.

Tesis

ZAMORA, Patricia Alexandra (2016): *Aplicación web gestora de inteligencia de negocios y el control en la inversión de campañas publicitarias a través de facebook en la empresa Kooper,* (tesis doctoral), Colombia ,Universidad de los Andes, Colombia.

Artículos en revistas

FERNÁNDEZ CALVO, Rafael (1996):« El tratamiento del llamado delito informático en el proyecto de ley orgánica de código penal: reflexiones y propuestas de la CLI (Comisión de Libertades e Informática)», Informática y derecho, n.12, págs. 1149-1162.

FUMERO, Antonio (2010): «Cultura y vida cotidiana en Iberoamérica, una revisión crítica más allá de la comunicación», Razón y Palabra, Revista Electrónica en América Latina Especializada en Comunicaciónnúmero 73, Agosto-octubre 2010.

G. A. Guadalupe (2015): «Inbound marketing en Linkedln para la gestión de marca», La Revista Icono 14, Volumen 13 Nº 1.

SARZANA, Carlos: «Criminalitá e tecnología. Computer Crimes», Rassegna *Penitenciaria* e Criminologica, vol.1, n. 1-2.

Artículos en línea:

1.Armando Corbin, Juan (2017): «Los 10 tipos de Redes Sociales y sus características», en: https://psicologiaymente.com/social/tipos-de-redes-sociales

2.Ciberdelincuencia en Argelia: el "escándalo" como el arma más poderosa de los perpetradores» (2018), الجريمة الإلكترونية بالجزائر- "الفضيحة" أعتى أسلحة الجناة (artículo original) en https://www.dw.com/ar%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9 42522945.

3. ERTZAINTZA: «Prevención frente a la delincuencia informática» [en línea] [consultado el 11 de marzo de 2012] Disponible en: http://www.ertzaintza.net/public/wps/portal/ertzaintza/

4. Genbeta social media (2017): «Instagram lanza nuevas utilidades para perfiles de empresas», en Miguel Ángel Sánchez Jiménez (2018): «Origen y evolución de internet y su desarrollo como entorno de interacción social a través de los medios sociales digitales», disponible en https://www.researchgate.net/publication/326305339

5. Ponce, V. y Maldonado, A. (2016). "Redes Sociales: Definición", recuperado el 9 de julio de 2017 en: http://recursostic.educacion.es//observatorio/web/ca/internet/web-20//1043-redes-sociales?start=1

RINALDE Paola (2000) **« ¿**De dónde viene el delito cibernético? Origen y evolución del delito cibernético», disponible en https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

6. https:// www.rae.es/diccionario-de-la-lengua-espanola/la-23a-edicion-2014

Anexos

- **Encuesta**

Con el fin de la elaboración de nuestra tesina de master titulada "Las redes sociales y el peligro de los delitos informáticos", nos gustaría que usted pudiera responder a las siguientes preguntas.

Edad:…….

Género: ……..

Masculino ☐ Femenino☐

Pregunta 1:¿Eres un usuario de las redes sociales?

Sí ☐ No ☐

Pregunta 2: ¿Qué son las redes que más utilizas?

Facebook ☐ Instagram☐ Snapchat☐ twitter☐ whatsApp☐

Pregunta 3: ¿Con qué frecuencia usas esta red por el día?

Menos de tres horas☐ de 3 a 5 horas☐ más de 5 horas☐

Pregunta 4: ¿Para qué utilizas esta red?

Ocio☐ Chat ☐ aprendizaje☐ economía ☐ Publicidad☐ otro motivo☐

Pregunta 5: ¿Qué información sueles exponer en tu perfil? (varias opciones)

Sexo☐ Fecha de nacimiento☐ Tu número de teléfono☐ Tu dirección☐ email☐ Los miembros de tu familia☐ Tus actividades☐ Religión☐ Opinión personal ☐

Pregunta 6 : Los datos personales que proporcionas en tu perfil son:

- Verdaderos☐
- Falsos ☐

Pregunta 7: A quién añades a tus listas de amigos? (varias respuestas posibles)

- Los amigos que conozco en la vida real☐
- Los amigos de mis amigos☐
- Todo el mundo, lo conozca o no☐
- Miembros de mi familia☐
- Otros:……

Pregunta 8: ¿Quién puede consultar tu perfil?

- Solamente tus amigos ☐
- Tus amigos y los amigos de estos ☐
- Todo el mundo☐
- Sólo a quien das permiso para visitar tu perfil ☐

Pregunta 9:¿Cuáles de las siguientes tecnologías sueles utilizar para conectarte y consultar tus cuentas personales?

- Teléfono móvil☐
- Tablet☐
- Ordenador de mesa☐
- Ordenador portátil☐

Pregunta 10: ¿Crees que estás seguro al momento de utilizar la red o uno de estos medios tecnológicos?

Sí☐ No☐

Pregunta 11¿Sueles revisar las opciones de "privacidad" y "seguridad" de las redes sociales antes de crear cuentas y perfiles?

Sí☐ No☐

Pregunta 12: ¿Conoces algunas técnicas de seguridad informática?

Sí☐ No☐

- En caso afirmativo, cita ejemplos

……
……
……

Pregunta 13:¿Fuiste alguna vez víctima de un delito informático?

Sí☐ No☐

Pregunta 14 :¿Qué se te pidió a cambio?

Dinero ☐ otra cosa ☐

Pregunta 15:¿Sigues poniendo cierta confianza en esta red?

Sí☐ No☐

Pregunta 16: ¿Cómo tenemos que reaccionar ante un delito informático que afecta nuestra identidad? (varias opciones)

- Realizar la denuncia para que el delincuente se sancione jurídicamente☐
- Desconectar de internet los aparatos utilizados☐
- Bloquear las cuentas ☐
- Borrar los archivos☐

Guerre à la piraterie

Le siège de l'APS a abrité hier, une conférence sur "la cyber sécurité : enjeux réels et stratégies en Algérie" animée par M. Abdelaziz Derdouri, directeur général de la SSRI.

La cyber sécurité est définie comme la protection des réseaux contre la menace des intrusions pirates grâce à des mesures de prévention pour juguler les risques et les préjudices dangereux pour la sécurité nationale.

Qu'arriverait-il, selon M. Derdouri, si les réseaux de distribution d'électricité, de transport, de défense, du commerce ne sont plus opérationnels ou fiables en raison d'attaques malveillantes ou criminelles ?

La cyber sécurité consiste en d'autres termes à protéger les systèmes informatiques des organismes vitaux contre les dégradations ou la destruction qui peuvent provoquer le ralentissement ou l'arrêt d'activité d'un pays.

L'évaluation de la menace s'effectue par exemple par l'intermédiaire des botnets (Robot Network) et Malwares (logiciel malveillant).

Très schématiquement un botnet est un ensemble de bots informatiques reliés entre eux. C'est un réseau de "machines-zombies" et toute machine connectée à internet est susceptible d'en être la cible. Quant au Malware, il peut être défini en tant que logiciel malveillant que l'on développe pour nuire à un système informatique. Il y a 4.000 à 6.000 botnets opérationnels aujourd'hui.

Botnets et Malwares sont devenus des affaires commerciales. Ils ne sont pas à l'abri de pratiques délictueuses. Le botnet, à titre d'exemple, relaie des spasms pour le commerce illégal, il peut affecter d'autres machines par diffusion de virus.

Même s'ils ne sont pas souvent déclarés, le conférencier avance le nombre de 3.000 incidents en 2009.

Il cite quelques pays dangereux d'où émanent les attaques. Les USA, la Chine, la Russie, la France, l'Iran...

S'agissant des risques pour l'année 2010, M. Abdelaziz Derdouri évoque l'augmentation du nombre d'attaques contre les points sensibles, le non-respect des consignes de sécurité, l'insuffisance des ressources. Quant aux menaces internes, il cite les cas d'accès aux sites sociaux, les pertes ou vols des équipements.

Les secteurs les plus attaqués demeurent l'information, les télécommunications, les institutions gouvernementales, les banques.

Il existe une cybernétique de la guerre. L'orateur parle de guerre psychologique. Une arme cybernétique coûte beaucoup moins cher qu'un avion de combat par exemple.

La guerre cybernétique, selon un responsable de l'OTAN, est un problème global, facilement déployable et très difficile à localiser.

A partir du moment où la cybercriminalité englobe toute les infractions susceptibles de se commettre sur un système informatique connecté à un réseau, se pose fatalement le problème de la sécurité des technologies de l'information et de la communication. La croissance exponentielle de tous ces matériels induit la nécessité de protéger les données et les ressources. M. Abdelaziz Derdouri énumère brièvement les dispositifs juridiques de la France et des USA. Il évoque l'Algérie qui a adopté une loi contre la cybercriminalité en 2009, qui vise à prévenir les infractions informatiques.

La cyber sécurité, à travers les enjeux qu'elle met en place et les stratégies qu'elle mobilise demeure indéniablement, un problème de sécurité nationale. L'orateur évoque pour ce qui concerne notre pays, des initiatives qui sont prises dans ce sens, mais il reste à faire pour développer notre propre logiciel.

De même que les choix technologiques rendent nécessaire une politique nationale des nouvelles technologies pour défendre nos entreprises et l'intérêt de notre pays d'une manière générale.

Mohamed Bouraïb

Journal el moudjahid, numéro : 13886.

"النهار" تنشر القصة الكاملة لأغرب قضية تعالجها العدالة الجزائرية

"هاكر" من باتنة يدوّخ أمريكا ومكتب تحقيقاتها الفيدرالي!

في أول قضية قرصنة إلكترونية تطرح على مستوى العدالة الجزائرية، نظرت نهار أمس محكمة الجنح لباتنة في ملف الهاكر "ع.ي" 21 سنة، الذي وجهت له تهمة البحث والتجميع والنشر والإتجار في معلومات إلكترونية بطريقة غير قانونية، وسط دهشة كل من كان في قاعة المحاكمة من متهمين، عناصر شرطة، محامين، مواطنين وحتى القاضي وممثل الحق العام.

سعيد حريقة

حيث ساد جو من الهدوء الكبير والإنتباه الشديد لتفاصيل المحاكمة من بدايتها إلى نهايتها دون كلل أو ملل كما جرت العادة، خاصة أثناء استجواب المتهم وطبيعة الأسئلة والأجوبة التي ورغم أن معظم من كان داخل القاعة لم يفهم فيها شيئا، إلا أن الإنتباه بقي سيد الموقف إلى النهاية، ذلك لأن أسئلة القاضي وممثل الحق العام كانت تتمحور حول أمور غير مألوفة لدى عامة المواطنين، والمألوفة منها كانوا يقرؤونها في الجرائد أو يسمعون عنها عبر أمواج الإذاعة وشاشات التلفزيون، باعتبار أنها كانت تتمحور حول مكتب التحقيقات الفيدرالي الأمريكي والأتراك، والروس والإنجليز، وكبرى الشركات الأمريكية الخاصة بتطوير منظومات حماية المواقع الإلكترونية والقرصنة وبيع وشراء المعلومات عبر العالم الإفتراضي والأنترنت عن طريق المساومة والإبتزاز، وكان المتهم الذي بدت على وجهه ملامح التخلق والطيبة والسلوك السوي والذكاء الخارق، يجيب على جميع أسئلة القاضي بثقة وهدوء كبيرين، مفندا التهمة التي وجهت له، وموضحا أنه كان فقط يقوم ببيع أنظمة معلومات خاصة بحماية المواقع الإلكترونية، ويقوم بخدمات إشهارية لصالح أصحاب المواقع الإلكترونية الراغبة في ذلك، نظير تلقيه أموال مقابل هذه الخدمات، إلا أن القاضي كان يؤكد أن المتهم يقوم بالدخول إلى مواقع شركات أمريكية ويستولي على معلوماتها السرية، قبل أن يساومها من جديد بدفع أموال مقابل استرجاع تلك المعلومات، كما أكد القاضي أن المتهم يقوم ببيع تلك المعلومات لقراصنة من أستراليا، أوروبا الغربية، روسيا وتركيا، وهو ما أكدته الخبرة المنجزة من طرف الشرطة العلمية، والتي تلا تفاصيلها ضرطي خبير قال إن المتهم وباستعمال بريده الإلكتروني الحامل لاسم مستعار يعني بالعربية "القبعة البيضاء"، قام باقتحام موقع شركة "سافت نات وورك" الأمريكية المختصة في توفير الحماية لمختلف المواقع الإلكترونية، واستولى على معلومات سرية لزبائنها وساوم القائمين على الشركة بدفع مقابل مالي نظير استرجاع تلك المعلومات، وأن المتهم كان يقوم ببيع معلومات سرية خاصة بزبائن مواقع أخرى مقتحمة لقرصانين روسي وتركي وآخر جزائري مقيم في إنجلترا، مقابل مبالغ مالية ترسل إليه عن طريق حوالات بريدية عبر مؤسسة « ويسترن يونيون » العالمية، وحسب قاضي الجلسة فإن بداية كشف القضية كانت بعد شكوى شركة "سافت نات وورك" لمكتب التحقيقات الفيدرالي الأمريكي "أف بي آي"، تفيد بأن موقعها تعرض إلى قرصنة من قبل « هاكر » مجهول، تبين أنه جزائري بعد استعمال طرق علمية وتقنية متطورة، وهي الشكوى التي طلب من خلالها البوليس الدولي المساعدة من طرف الشرطة الجزائرية، هذه الأخيرة وفي إطار اتفاقيات تعاون دولية وباستعمال طرق تقنية كذلك واستغلالا للبريد الإلكتروني الذي كان يتعامل به القرصان، تم تحديد مكان هذا الأخير الذي حيّر أمريكا ودوّخ مكتب تحقيقاتها، وهو الشاب الباتني البالغ من العمر 21 سنة المدعو "ي.ع" القاطن في حي بوزوران وسط مدينة باتنة، والذي كان يقوم بكل تلك العمليات من غرفة مسكنه، قبل أن يلقى عليه القبض وتحجز في غرفته حوالات بريدية مختلفة وأقراص مضغوط يحمل معلومات سرية خاصة بالشركة الأمريكية "سافت نات وورك"، وبعد بحث تحقيقات معمقة على أعلى المستويات على محكمة الجنح، التي أدانته نهار أمس عقب محاكمة فريدة من نوعها دامت ساعتين من الزمن بسنة حبسا نافذا وغرامة مالية مقدرة بخمسة ملايين سنتيم، بعد التماسات وكيل الجمهورية بتسليط عقوبة سنتين حبسا نافذا، وكان ممثل الحق العام الذي كان بدوره مندهشا لقوة تحكم المتهم، الذي لا يتعدى مستواه الدراسي السنة الثالثة ثانوي في الأنظمة المعلوماتية والإعلام الآلي، أشار إلى تواجد عدة مواقع شركات أمريكية اقتحمها الهاكر الباتني، ذكر منها ثلاثة مواقع فقط، وأنه عرض بيع 2000 معلومة بـ8 دولار مقابل المعلومة الواحدة، وذلك خلال أطوار الفتح المنصوب له من قبل الجهات المختصة، الأمر الذي نفاه المتهم تماما

وقال في شأنه إنه أراد فقط تصريف صاحب البريد الإلكتروني الذي عرض عليه فكرة شراء المعلومات المتواجدة بحوزته، وأضاف وكيل الجمهورية أن طبيعة هذه الجريمة التي تعالجها العدالة الجزائرية لأول مرة تعد سابقة من نوعها، وأن القانون الجزائري يجرم أفعالها وأن ما قام به المتهم يدخل في إطار التهمة الموجهة إليه، لذلك التمس إدانته بسنتين حبسا نافذا، هذا وكان دفاع المتهم المتكون من محاميين اثنين، قد ركّزا في مداخلتيهما على انعدام أدلة التجريم من ركن مادي ونية في الجريمة، خاصة بعد رفض أحد المحاميين الخبرة التي أتت بها العدالة عن طريق الشرطي الخبير، حين قال إنه من الطبيعي أن تكون الخبرة ضد المتهم في هذه الحالة، مطالبا من رئيس الجلسة تسجيل إشهاد رفض من قبل القاضي، مضيفا أن موكله قد يكون أخطأ بالدخول إلى الشبكة العنكبوتية، لكنه لم يقم البتة بقرصنة مواقع أمريكية أو بيع معلوماتها السرية، كما تساءل الدفاع عن الأضرار التي ألحقت بالشركة التي تعرضت إلى القرصنة، ملتمسا من هيئة المحكمة براءة موكله المنحدر من عائلة جد محترمة، كل أفرادها إطارات في الدولة الجزائرية، مستشهدا في خصوص المتهم أنه غير مسبوق قضائيا ما يدل على أنه مواطن صالح، وأنه مجرد هاوي للإبحار في عالم الأنترنت لا غير، كما أضاف الدفاع أن شكوى المؤسسة الأمريكية لم تقتصر فقط على موكله وإنما تعدت عدة دول عبر العالم، دون الإشارة إلى ما إن كانت هذه الشكاوى وراء القبض على الهاكر التركي صديق الهاكر الباتني المتواجد حاليا رهن الحبس مثلما قال ممثل الحق العام في مرافعته، وبناء على كل ذلك ولانعدام أركان الجريمة - حسب الدفاع - التمس تبرئة ساحة الشاب من التهمة الموجهة إليه، وحسب مجريات المحاكمة فإن المتهم كان يقوم بقرصنة مواقع إلكترونية منذ سنة 2006 وتحصل مقابل ذلك على حوالي 100 مليون سنتيم، ولأن والد المعني يعد من رجال الأعمال المعروفين فقد ساد اعتقاد وسط الحضور - حسب البعض منهم - أن يكون المتهم قد سقط ضحية شبكة هاكر عالمية، استغلت مهارته في التحكم في الإعلام الآلي لتحقيق أغراض مشبوهة، منها جني أموال طائلة مقابل إعادة بيع المعلومات المباعة لهم بمبالغ رمزية لنفس المؤسسات التي تعرضت إلى القرصنة، وهي الفرضية التي رجّحها قاضي الجلسة وكذا ممثل الحق العام.

بينها قضية استهداف موقع "الشروق أونلاين" وتخريبه من قبل مصريين

تحقيق في 800 اعتداء إلكتروني شنه "هاكرز"

فتحت الجهات القضائية المختصة تحقيقات معمقة في 800 قضية متعلقة بالجريمة الإلكترونية منذ دخول قانون مكافحة الجريمة الإلكترونية حيز التنفيذ السنة المنقضية، حيث تورط في هذه القضايا جزائريون وأجانب استهدفوا شبكات وبنوك المعلومات المركزية لمؤسسات جزائرية ومتعددة الجنسيات.

كشف، أمس، عبد العزيز دردوري رئيس مدير عام مؤسسة الأمن المعلوماتي وأمن شبكات الاتصال على هامش إلقائه محاضرة حول "الأمن المعلوماتي والجريمة الإلكترونية" بمركز الدراسات الإستراتيجية لجريدة "الشعب" بالجزائر العاصمة، عن فتح الجهات القضائية المختصة بالتنسيق مع خبراء المعلوماتية المعتمدين من قبل وزارة العدل تحقيقات معمقة في 800 قضية متعلقة بالهجمات الإلكترونية التي استهدفت شبكات وبنوك معلومات مؤسسات حساسة وكذا تخريب مواقع إلكترونية عن طريق القرصنة الرقمية.

وأوضح صاحب مؤسسة الأمن المعلوماتي وأمن شبكات الاتصال الجزائرية أن العدد الحقيقي للهجمات الإلكترونية التي تتعرض لها المواقع الجزائرية وشبكات وبنوك معلومات المؤسسات الجزائرية غير محدد بدقة لأن الكثير من ضحايا هذه الهجمات لا يصرحون بها أو حتى أنهم لا يتفطنون لعملية القرصنة الإلكترونية واختراق قواعد بياناتهم من قبل الغير، مضيفا أن الحكومة الجزائرية مطالبة بوضع تشريعات وقوانين كافية لحماية مستعملي الأنترنيت وأصحاب المواقع الإلكترونية وبنوك المعلومات وشبكات الاتصال من الاختراق والقرصنة، فضلا عن تكثيف دورات التوعية والتكوين لرفع مستوى الوعي والمعرفة الرقمية.

وذكر المتحدث أن الجريمة الإلكترونية والقرصنة الرقمية كبدت العالم خلال سنة 2008 خسائر مالية تجاوزت 100 مليار دولار، مشيرا إلى أن كل من الولايات المتحدة الأمريكية وروسيا والصين تعتبر الدول الأكثر خطورة في مجال تهديد أمن المعلومات، في حين تمثل كل من نيجريا وغانا وجنوب إفريقيا والكاميرون الدول الأخطر في الجريمة الإلكترونية على مستوى القارة الإفريقية ما يستدعي على الجزائر تعزيز أمنها المعلوماتي من خلال خطة حكومية تؤمن مختلف المؤسسات والهيئات خاصة في ظل تحضير الجزائر لإطلاق مشروع الحكومة والتجارة الإلكترونية.

كما أثارت قضية اختراق موقع "الشروق أونلاين" ومحاولة الاستيلاء عليه وتخريبه من قبل جهات مصرية نقاشا واسعا على هامش الندوة باعتبارها أكبر قضية مست الأمن المعلوماتي لمؤسسة جزائرية، حيث تعرض موقع "الشروق أونلاين" أكبر موقع إلكتروني جزائري من حيث عدد الزيارات والمشاهدة شهر مارس المنقضي إلى هجمة الكترونية مصرية تم فيها الاستيلاء على اسم النطاق ومرر القراصنة المصريون رسائل عبر الموقع قبل أن تسترجعه مؤسسة "الشروق" للإعلام والنشر بعد تكثيف الاتصالات مع المؤسسة الأمريكية المكلفة بإيواء الموقع ورفع شكوى للسلطات الجزائرية قصد التحقيق في حيثيات القضية.

• زين العابدين جبارة

جريدة الشروق اليومي العدد 2945

الخميس 06 ماي 2010 / الموافق لـ 21 جمادى الأولى 1431 هـ / العدد 2925

99 بالمائة من مرتكبي الجرائم المعلوماتية تقنيون أو طلبة

3 آلاف هجمة شهريا للهاكرز على المواقع الإلكترونية في الجزائر

• تجربة "إختطاف" موقع الشروق وهيئات رسمية بينها الرئاسة والجمارك أعادت الحسابات

كشفت إحصائيات قدمها مركز البحوث القانونية والقضائية التابع لوزارة العدل أن عدد الهجمات اليومية على مختلف المواقع الإلكترونية في الجزائر وصل إلى 3000 هجمة في الشهر، مما يعني أن ظاهرة الجريمة المعلوماتية بدأت تعرف انتشارا بعد بداية استعمال تكنولوجيات الإعلام والإتصال الحديثة في جميع المجالات، وحسب إحصائيات المركز فإن عدد الجرائم المعلوماتية تطور من 12 قضية سنة 2005 تتضمن 20 متهما إلى 12 قضية تتضمن 51 متهما سنة 2006، وإلى غاية أفريل 2010 بلغ عدد الأشخاص المتابعين في الجرائم المعلوماتية 88 شخصا.

جميلة بلقاسم

■ الجرائم الالكترونية من الهواية الى المهنة

وأكدت نفس المصادر أن الجرائم المعلوماتية المنتشرة في الجزائر تتمثل في هجمات على مواقع إلكترونية جزائرية منها مواقع رسمية وخاصة، وقال مدير المركز أن عقوبة المتورطين في تدمير وتخريب المواقع الإلكترونية تصل إلى 3 سنوات سجنا في القانون الجزائري، غير أنها قد تكون أكثر إذا تعلق الأمر بمواقع رسمية تابعة للدولة أو مواقع تهدد الأمن الوطني للبلاد، كما سجل المركز حالات تتمثل في الدعاية الخادعة والإرهابية، وسرقة المعلومات عبر الانترنيت، من خلال التوغل في قاعدة المعطيات، والمساس بالحياة الخاصة، وسجل كذلك تدمير وتحويل مواقع هيئات وجرائد وطنية بينها موقع جريدة "الشروق"، وسجل أيضا استعمال الموقع الإلكتروني لبيع قطع أثرية بولاية عنابة، وعرض صور خليعة على الأنترنيت، واختراق منظومة البنك الجزائري والجمارك الوطنية من طرف شاب يتحكم في الإعلام الآلي من ولاية أم البواقي، كما تنتشر جرائم أخرى تتمثل في تفكيك شفرات القنوات التلفزيونية المشفرة بطريقة غير نظامية.

وتتمثل القضايا المسجلة في 13 قضية خاصة بالدخول غير المشروع مع إتلاف المعطيات أو تعديلها، و11 قضية تتعلق بالدخول غير المشروع، و8 قضايا إدخال معلومات خلسة، و3 قضايا حيازة معطيات متحصل عليها من دخول غير مشروع، وقضيتين تتعلقان بالمتاجرة في معلومات متحصل عليها من دخول غير مشروع ويمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وقضية واحدة خاصة بنشر صور للإستغلال الجنسي للأطفال، و99 بالمائة من مرتكبي هذه الجرائم هم تقنيون أو طلبة.

وقال المدير العام لمركز البحوث القانونية والقضائية جمال بوزرتيني في تصريحات للصحافة على هامش الملتقى الدولي حول محاربة الجريمة المعلوماتية أنه من حسن حظ الجزائر أنها ماتزال لا تعمل ببطاقات الدخول إلى الحسابات البنكية وماتزال لا تتوفر على الانترنت ذي التدفق العالي، غير أنه بعد 2013، حيث ستكون الانترنت ذات السرعة الفائقة متوفرة سيكون الأمر أخطر بكثير مما هو عليه ولا بد من اتخاذ الإحتياطات الضرورية.

وكشفت تقارير التي عرضها المركز في الملتقى أن الجزائر ليست في منأى عن الجريمة المعلوماتية، حيث يعتبر هذا الشكل الجديد من الإجرام العابر للحدود تهديدا حقيقيا للمؤسسات والشركات مما يستدعي ضرورة إنشاء جهاز للمحاربة والوقاية.

وحسب المدير العام للمركز فإن الجزائر قامت بتكييف الجهاز الأمني والقضائي بطريقة تمكنها من التحكم في محاكمة هذا النوع من الجرائم، حيث تم على مستوى أمن كل الدوائر عبر الوطن إنشاء فرقة متخصصة من الشرطة القضائية مهمتها التحقيق في الجرائم الإلكترونية، كما ينتظر أن يتم قريبا إصدار النص التنظيمي لقانون مكافحة الجريمة المعلوماتية الذي صادق عليه البرلمان بغرفتيه مؤخرا، في حين تم على مستوى جهاز العدالة تكوين قضاة متخصصين في الجرائم المعلوماتية في الولايات المتحدة الأمريكية، ومن المنتظر أن يتم قريبا تنصيب هيئة مختصة في مكافحة الجريمة الإلكترونية.

وكشفت إحصائيات مدير المركز أنه يوجد في الجزائر 4,5 مليون متصفح للأنترنت منهم 40 بالمائة يقضون 3 ساعات يوميا أمام الانترنت، وأن 74 بالمائة من مستعملي الانترنت هم رجال، و25 بالمائة نساء، وتعتبر الفئة العمرية التي يتراوح سنها بين 20 و29 سنة الأكثر تصفحا للأنترنت في الجزائر.

جريدة الشروق اليومي العدد2925

Consecuencias producidas por el Cyber Bullying

- Existen muchas consecuencias , por el cyber bullying, que en algunos casos pueden llegar hasta causar la muerte.
- Pero la principal consecuencia de el cyber bullying es el daño psicológico que recibe la victima.


SEXTORSIÓN
Chantaje en el que alguien, utiliza estos contenidos para obtener algo de la víctima, amenazando con su publicación.
Tengo tu foto
Dame $1.500 o la subiré a las redes
¡No, por fa! espera

العنوان: وسائل التواصل الاجتماعي وخطر الجرائم الالكترونية.

ملخص: هذا البحث يتطرق الى استخدام وسائل التواصل الاجتماعي و دورها في الحياة الشخصية والمهنية لمستخدمي الانترنيت و يسلط الضوء على الأخطار المسمات الجرائم الإلكترونية التي ولدت من سوء استخدام وسائل التواصل الاجتماعي ،حاولنا دراسة المشكلة بعمق و تقديم نصائح ومعلومات تحسيسية لتفادي الوقوع كضحية لهاته الأعمال اللاأخلاقية

الكلمات المفتاحية: شبكات التواصل الاجتماعي، جرائم الكمبيوتر، مجرم الكتروني

Titre: Les réseaux sociaux et le risque de cybercriminalité

Résumé:

Ce travail de recherche porte sur l'utilisation des réseaux sociaux et sa présence dans la vie personnelle et professionnelle des citoyens, mettant en lumière les dangers appelés cybercriminalité généré par leur utilisation abusive. On a essayé d’étudier ce probléme en profondeur, en suggérant certaines solutions et informations pour éviter d'être victime de ces pratiques contraires à l'éthique.

Mots clés: réseaux sociaux, délits informatiques, cyber-aligneurs.

Title: Social media and the risk of cybercrime

Summary: This research work deals with the use of social media and it's presence in the personal and professional lives of citizens, shedding light on the dangers called reported crime, generated by their misuse. We have tried to study this problem by suggesting certain solutions and information to avoid being a victim of these unethical practices.

Keywords: social networks, computer crimes, cyber-aligners.