South American Publishing

SAP Netnography. 2024; 2:98
doi: 10.62486/net202498

REVIEW

Criminal profiling of cybercriminals: Analysis on motivations and traits of hackers

Perfilación criminal de los ciberdelincuentes: Análisis sobre motivaciones y rasgos de los hackers

Rocío Magalí Méndez[1], María Inés Lanza[1]

[1]Universidad Siglo 21, Licenciatura en Criminología y Seguridad. Bahía Blanca, Buenos Aires. Argentina.

Cite as
Méndez RM, Lanza MI. Criminal profiling of cybercriminals: Analysis on motivations and traits of hackers. SAP Netnography. 2024; 2:98. https://doi.org/10.62486/net202498

Publication History
Submitted: 28-05-2024
Revised: 01-09-2024
Accepted: 22-12-2024
Published: 23-12-2024

ABSTRACT

The present research conducted an approach to the criminal profiling of cybercriminals, based on the analysis of criminal behavior and statistics of hackers. This descriptive and explanatory analysis, carried out through interviews, surveys, and data collection from cybercrime victims, news, and laws, examined various behaviors, patterns, and traits of hackers. It was possible to conclude the lack or outdated nature of legal regulation on the subject. It is necessary to update our legislation to adapt to the technological changes that occur every day. Despite the fact that the inherent characteristics of cybercrimes involve occurrences in an intangible space, getting to know the types of individuals who commit them could help in preventing them.

Keywords: Hackers; Cybercrimes; Cybercriminals; Technology.

RESUMEN

La presente investigación, realizó una aproximación a la perfilación criminal de los ciberdelincuentes, basado en el análisis de la conducta criminal y estadísticas de los hackers. Este análisis descriptivo y explicativo, realizado en base a entrevistas, encuestas y recopilación de datos obtenidos de víctimas de la ciberdelincuencia, noticias y leyes, examinó las distintas conductas, patrones y rasgos de los hackers. Se pudo concluir la falta o desactualización de regulación legal en la temática. Es necesario actualizar nuestra legislación para que se adapte a los cambios tecnológicos que se desarrollan día a día. Más allá de que las características propias de los delitos informáticos es que ocurran en un espacio intangible, el hecho de acercarnos a conocer los tipos de personas que los realizan podría ayudar a prevenirlos.

Palabras clave: Hackers; Ciberdelitos; Ciberdelincuentes; Tecnología.

© 2024; The Authors. This Open access article is distributed under the Creative Commons Attribution 4.0 license (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

INTRODUCCIÓN

El análisis del comportamiento criminal, en tanto especialidad novedosa, se construyó con base en distintos aportes realizados por la criminología y las ciencias de la conducta aplicados al campo de la práctica criminalística. El uso de la psicología para comprender y prevenir la criminalidad debe considerarse desde los orígenes de la ciencia psicológica.

La construcción de perfiles psicológicos se basó principalmente en la consideración, empleo y desarrollo de clasificaciones propias de la psiquiatría, lo que terminó encasillando a delincuentes en posibles diagnósticos de enfermedades mentales. Con el paso del tiempo, se desarrollaron distintas teorías que comenzaron a considerar otro tipo de factores más allá de los psicológicos y que son fundamentales para una aproximación más precisa y certera del perfil de un criminal.

Son múltiples las metodologías, desarrollos y definiciones conceptuales que comienzan a surgir. Ressler considera los aportes realizados desde los Estados Unidos y señala que el perfil criminal ha sido descrito como una suma de pistas, como un intento de recopilar información específica y como un esbozo biográfico de patrones de conducta. Por otro lado, Holmes et al. consideran tres objetivos principales que se desprenden del análisis y estudio psicológico del delincuente:

1. Aproximación a una valoración desde la criminología social y psicológica de la personalidad del delincuente.
2. Consideración de las inferencias posibles en relación a las pertenencias del delincuente halladas en las distintas escenas del crimen.
3. Sentar las bases de posibles focos de indagación e hipótesis claves en la investigación penal.

Estos autores plantean que no todos los casos son analizables. En este contexto, entonces, la perfilación criminal busca generar una aproximación a las características del presunto agresor, lo que permite disminuir el espectro de la investigación y centrarse en aspectos más certeros y definidos.

Siguiendo a Velasco de la Fuente, la técnica puede ser aplicada en casos de serialidad, sobre todo en delitos violentos, ya que la repetición posibilita determinar la presencia o no de una pauta o patrón de conducta, lo que conlleva una elevada movilización social y una pronta intervención.

La metodología para la construcción de un perfil criminal consiste en analizar y evaluar distintos aspectos:

- La escena del crimen es el lugar y espacio que el delincuente ha escogido para cometer un crimen.
- El modus operandi hace referencia al método o forma de operar. Considera, principalmente, la manera o método que el agresor ha empleado para cometer el delito. De su análisis, se recoge información acerca de cómo actúa ese criminal, lo que hace posible delimitar y aproximarse a las características psicológicas deducibles de su forma de actuar.
- El estudio detallado de la información que brinda el modo de operar de los delincuentes permite definir indicios
- La firma, para Robert Keppel, constituye una parte de la escena del crimen que involucra distintas expresiones de las fantasías del criminal, es decir, es el conjunto de acciones que no son necesarias para cometer el delito. La firma tiende a ser uno de los patrones principales que posibilitan el establecimiento de la serialidad en distintos hechos, siendo posible la adjudicación de estos a un único autor.
- El análisis de delitos seriales se complementa con el análisis geográfico. Existen diversas teorías que explican el comportamiento espacial del autor de un hecho con finalidad de establecer la existencia o no de una relación entre estos lugares y las rutinas del victimario. Este perfil describe la conducta espacial y los terrenos donde se desplaza el delincuente, las escenas del crimen, los puntos de anclaje de los hechos delictivos, zonas de riesgo, base de operaciones, etc.

El objetivo de esta investigación es desarrollar el perfil criminal de los ciberdelincuentes, en particular de los “hackers”. Realizar un análisis exhaustivo de la literatura y las leyes que regulan este tipo de crímenes, identificar las principales tendencias y brechas en la investigación, recopilar y analizar datos de entrevistas a “hacker éticos”, realizar un análisis cuantitativo, analizar las implicaciones éticas de la investigación y contribuir al conocimiento existente, para identificar y establecer un perfil psicológico de los hackers para descubrirlos y prevenir sus crímenes tempranamente.

La Justicia Argentina define al ciberdelito como conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas. Consiste en estafas, robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como cyberbulling, grooming, phishing cometidos por ciberdelincuentes que actúan en grupos o trabajan solos.[1]

En cuanto a las leyes que abordan la temática de la ciberseguridad en el país se pueden mencionar:

- Ley 26.388 de Delito informático: Establece las penas por los delitos de divulgar fotos de menores de 18 años, para quien accediere indebidamente a una comunicación electrónica, quien accediere a un sistema o dato informático de acceso restringido, para quien defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. La última modificación de esta ley fue en el año 2008. Quedando muy desactualizada para nuevos métodos de acceso a los datos.
- Ley 25.326: Ley de protección de datos personales, habeas data. Tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre. Cuya última modificación fue en el año 2000.
- Ley 25.506: Ley de firma digital. Reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley. Sancionada en 2001.
- Ley 26.904. Ley de Grooming. Establece las penas para quien, por medio de comunicaciones electrónicas,

telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma. Fue sancionada en el 2013 y es la l e y más actual en temática de ciberdelincuencia.

Otras normativas a mencionar son:

- Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.
- Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información.
- Resolución 1523/2019. Definición de Infraestructuras Críticas.
- Decreto 577/2017. Creación del Comité de Ciberseguridad.
- Decreto 480/2019. Modificación del Decreto 577/2017.
- Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad.
- Resolución 141/2019. Presidencia del Comité de Ciberseguridad.

El ciberespacio es un área intangible a la que cualquier persona puede acceder con una computadora desde su hogar, su lugar de trabajo o dispositivos móviles. Los ciberdelincuentes usan medios tecnológicos como: internet, computadoras, celulares, redes de comunicación 3G y 4G, redes de fibra óptica y software.

El ciberdelito puede llegar de muchas maneras: sitios web no seguros, redes sociales, agujeros creados por vulnerabilidades de seguridad, contraseñas poco seguras en cuentas y dispositivos inteligentes y, sobre todo, el correo electrónico.

Los ciberdelitos se cometen a través de programas maliciosos desarrollados para borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin tu autorización y con fines económicos y de daño. Algunos ejemplos son:

- Ataques en tu navegación: desvían tu navegador hacia páginas que causan infecciones con programas malignos como virus, gusanos y troyanos. Estos programas pueden borrar tu sistema operativo, infectar tu teléfono y tu computadora, activar tu webcam, extraer datos, etc.
- Ataques a servidores: pueden dañar o robar tus datos y negarte el acceso a tu información.
- Corrupción de bases de datos: interfieren en bases de datos públicas o privadas para generar datos falsos o robar información.
- Virus informáticos: encripta archivos, bloquean cerraduras inteligentes, roban dinero desde los celulares con mensajes de texto que parecen de la compañía.
- Programa espía: alguno de los dispositivos tiene instalado un software que le permite encender y grabar con la cámara y el micrófono. También puede acceder a tu información personal sin autorización y sin que lo sepas.

Los ciberdelincuentes usan la ingeniería social para engañar, amenazar y obtener datos personales o información de otras personas u organizaciones, obtener dinero, suplantar identidades, acoso digital y sexual. Algunos ejemplos son:

- Phishing o vishing: los ciberdelincuentes se hacen pasar por empresas de servicios, oficinas de gobierno o amigos de algún familiar y te piden los datos que les faltan para suplantar tu identidad y así operar tus cuentas en bancos, perfiles en las plataformas y redes sociales, servicios y aplicaciones web.
- Ciberbullying: es el acoso por mensajería instantánea, stalking en WhatsApp, Telegram, Facebook Messenger y en las redes sociales con la intención de perseguir, acechar, difamar y atentar contra el honor e integridad moral de una persona. Esto lo hacen a través del descubrimiento y revelación de secretos, de la publicación de comentarios o videos ofensivos o discriminatorios, de la creación de memes o el etiquetado de tus publicaciones.
- Grooming: se trata de personas adultas que, de manera velada, intentan obtener fotografías o videos sexuales de personas menores para posteriores chantajes o previo al abuso sexual.
- Sextorsión: consiste en pedir dinero a cambio de no difundir en las redes imágenes generadas para un intercambio erótico consentido.
- Ciberodio: son contenidos inapropiados que pueden vulnerar a las personas. Se considera ciberodio a la violencia, mensajes que incitan al odio, la xenofobia, el racismo y la discriminación o el maltrato animal.
- Pornografía infantil: se trata de la corrupción de personas menores y su explotación sexual para producir, comercializar imágenes y videos de actividad sexual explícita.
- Espionaje ilícito sobre las comunicaciones privadas de los ciudadanos.
- Violación a la intimidad por parte de las empresas proveedoras de servicios de internet sin el consentimiento del usuario, para conocer sus gustos y preferencias y establecer la venta agresiva de productos y servicios asociados.
- Acceso ilegal a las comunicaciones privadas de un trabajador (correos electrónicos, redes sociales, etc.)

Durante los últimos años hemos sido testigos del aumento de la aceleración en el proceso de adopción de nuevas tecnologías,

en particular luego de los largos periodos de aislamiento debidos a las medidas de profilaxis por la pandemia del COVID-19, que hizo que mucha gente tuviera que comenzar a trabajar a través de dispositivos informáticos en forma casi total, y en muchos casos sin los elementos de prevención ni la capacitación necesaria para prevenir las tipologías de delitos mencionados. Investigar el perfil criminal de los hackers es intrigante para la sociedad actual por varias razones. En primer lugar, permite una comprensión más profunda de las motivaciones que impulsan a algunas personas a participar en actividades delictivas en línea. Esto es esencial para desarrollar estrategias de prevención efectivas y políticas de seguridad cibernética. Además, un estudio en profundidad de estos perfiles puede contribuir significativamente a mejorar la ciberseguridad en un mundo cada vez más digitalizado. El conocimiento de cómo piensan y operan los hackers criminales es esencial para fortalecer las defensas de las organizaciones y proteger mejor los sistemas y datos sensibles. También es importante destacar que investigar el perfil de los hackers criminales puede ayudar a identificar tendencias y patrones en sus actividades delictivas. Esto puede ser de gran utilidad tanto para las fuerzas del orden como para las agencias de seguridad cibernética, ya que les permite adaptar sus estrategias para combatir amenazas en línea de manera más efectiva. Además, contribuir a la comprensión del campo de la ciberseguridad es un beneficio adicional. Al documentar y analizar los perfiles criminales de los hackers, se puede enriquecer el conocimiento colectivo en este campo y ayudar a la comunidad a estar mejor preparada para enfrentar las amenazas cibernéticas en constante evolución.

Es fundamental recordar que cualquier investigación en este campo debe llevarse a cabo de manera ética y legal, respetando las leyes y regulaciones aplicables, así como la privacidad de las personas involucradas en las investigaciones. Además, debido a la naturaleza en constante evolución de la ciberseguridad, es esencial mantenerse actualizado sobre las últimas tendencias y amenazas en línea para realizar investigaciones efectivas y pertinentes.

Según la Asociación Argentina de Lucha Contra el Cibercrimen,[2] se observa una leve disminución de casos consultados en el año 2021 con respecto al año 2020. Durante el 2021, el CERT.ar registró un total de 591 incidentes informáticos, cifra que superó en un 261 % a la del 2020, cuando se registraron 226 incidentes. Por lo pronto, sólo 18 de los casos registrados en 2021 se encuentran abiertos por lo que aún se está trabajando en ellos. El resto de los 573 incidentes se encuentran cerrados. En el 2020 fue considerable la suba de casos respecto a los años anteriores, principalmente casos de fraude, robo de datos y extorsión digital debido a la cuarentena estricta decretada en el país en el segundo y tercer trimestre. En el 2021 un porcentaje importante normalizó su forma de trabajo habitual, otros lograron capacitarse en materia preventiva, como así también las diferentes campañas de concientización tanto gubernamentales, de organizaciones civiles y los medios de comunicación lograron en cierta forma un efecto positivo en la prevención.

En la Argentina, según la Caracterización de la Criminalidad Organizada publicada por la página oficial del gobierno argentino "argentina.gob.ar",[3] los delitos más comunes son: narcotráfico, tráfico de armas, venta ilegal de autopartes, contrabando de mercancía, lavado de dinero y los ciberdelitos.

El cibercrimen, ha crecido en importancia a medida que las computadoras se han vuelto parte central del comercio, el entretenimiento y el gobierno. Un cibercriminal no difiere a un criminal del mundo físico. Sin duda, algunas de las manifestaciones son nuevas, pero una gran cantidad de los delitos cometidos con o contra las computadoras sólo difieren en términos del medio utilizado. En el libro "El Rastro Digital del Delito: aspectos técnicos, legales, y estratégicos de la informática forense",[4] sus autores concluyen en cuanto a la informática forense; la dinámica de la evolución humana y su avance tecnológico, han aportado un nuevo paradigma en la materia, generando nuevas escenas del crimen de características virtuales que concurren con las físicas ; nuevas escrituras que no son sobre soporte de papel y a la que no es posible aplicarles el método scopométrico que tan buenos resultados ha dado a la Documentología. La digitalización de la información ha hecho que ya no se deba buscar un rastro de una huella con un reactivo químico o magnético, sino con complejas herramientas computacionales que buscan ese indicio escondido, ese rastro, en un código binario, un algoritmo.

Los criminales del mundo real tienen la decisión de cometer delitos, por lo que, ante un cambio en el paradigma de los hábitos de los ciudadanos, es de suponer que los criminales tendrían la motivación para mutar hacia el cibercrimen. Según la RAE un Hacker o Pirata Informático es una persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora. Afortunadamente no todos los hackers o piratas informáticos utilizan sus conocimientos de la misma manera, existen diferentes tipos de hackers.

La clasificación general está compuesta por tres tipos: Black Hat, Grey Hat y White Hat pero con el paso de los años ha ido diversificando los tipos hasta formar una larga lista, los principales serían:[5]

- Black Hat o también llamados Ciberdelincuentes. Estos hackers acceden a sistemas o redes no autorizadas con el fin de infringir daños, obtener acceso a información financiera, datos personales, contraseñas e introducir virus. Dentro de esta clasificación existen dos tipos: Crackers y Phreakers, los primeros modifican softwares, crean malwares, colapsan servidores e infectan las redes, mientras que los segundos actúan en el ámbito de las telecomunicaciones.
- Para los Grey Hat su ética depende del momento y del lugar, prestan sus servicios a agencias de inteligencia, grandes empresas o gobiernos, divulgan información de utilidad por un módico precio.
- White Hat o Hackers éticos, se dedican a la investigación y notifican vulnerabilidades o fallos en los sistemas de seguridad.
- Los Newbies no tienen mucha experiencia ni conocimientos ya que acaban de aterrizar en el mundo de la ciberseguridad, son los novatos del hacking.
- Los Hacktivista ha crecido en los últimos años en número, utilizan sus habilidades para atacar a una red con fines políticos, uno de los ejemplos más representativos sería Anonymous.

https://doi.org/10.62486/net202498

Otro tipo de Hackers

- Phreakers: Son hackers que se enfocan en manipular o explotar la tecnología de las telecomunicaciones, especialmente los sistemas telefónicos.
- Hackers de ingeniería social: Son hackers que utilizan técnicas de manipulación psicológica para obtener información confidencial o acceso a sistemas informáticos. Pueden utilizar tácticas como el engaño, la suplantación de identidad, la persuasión, y la manipulación emocional.
- Hackers de hardware: Son hackers que se enfocan en la manipulación o explotación de dispositivos físicos, como tarjetas de crédito, cámaras de seguridad, o sistemas de control industrial.
- Hackers de red: Son hackers que se enfocan en explotar vulnerabilidades en redes informáticas y sistemas de comunicaciones.

La seguridad informática implica no sólo el uso de contraseñas seguras y la actualización de software y antivirus, sino también la educación y concientización sobre las posibles amenazas. Los ciudadanos pueden tomar medidas simples, como evitar compartir información confidencial en redes sociales o utilizar contraseñas complejas, mientras que las organizaciones deben implementar políticas de seguridad y realizar evaluaciones de riesgo y pruebas de penetración para identificar posibles vulnerabilidades.

Una de las principales amenazas son los malwares (virus informáticos) especialmente uno que se conoce como Ransomware, un software malicioso que encripta los archivos de la computadora para luego pedir dinero o generalmente criptodivisas a cambio de devolver dicha información secuestrada.

Tanto empresas privadas como organizaciones del Estado son víctimas a diario. Algunos ejemplos de empresas y organismos públicos hackeados en los últimos años en nuestro país son: el Ministerio Publico Fiscal,[6] el CONICET,[7] el Senado de la Nación,[8] Migraciones,[9] el Correo Argentino,[10] PAMI,[11] entre otras.

En agosto del 2022 sufrió un ataque el sistema informático del Poder Judicial de la Provincia de Córdoba que afectó su página web oficial, los servicios digitales y las bases de datos que contienen los expedientes. Este hecho generó que la inversión tecnológica será prioridad para el Poder Judicial de Córdoba para el año 2023.[12,13,14]

MÉTODO

En el presente trabajo de investigación, se adoptará una metodología que se enmarca en un enfoque descriptivo y cualitativo. Este enfoque se ha seleccionado cuidadosamente debido a su idoneidad para el objetivo de nuestro estudio, que es comprender y analizar en profundidad el perfil criminal de los hackers.

La metodología descriptiva se centrará en la recopilación de datos de diversas fuentes para proporcionar una descripción detallada y precisa de los aspectos relevantes relacionados con los hackers criminales. Para ello, se llevará a cabo una revisión bibliográfica del área, investigando libros, artículos académicos y otros recursos que aborden temas relacionados con la ciberseguridad y el hacking.

Además de la revisión bibliográfica, se realizará una investigación en línea para rastrear y analizar publicaciones web relacionadas con el tema. Dado que el campo de la ciberseguridad y el hacking es altamente dinámico y se actualiza constantemente, esta investigación en línea permitirá capturar las tendencias y desarrollos más recientes en el ámbito de los hackers criminales.

Una parte fundamental de la metodología cualitativa consistirá en la realización de entrevistas a especialistas en convenciones y conferencias relacionadas con hackers y ciberseguridad. Estas entrevistas proporcionarán valiosa información de primera mano, insights y perspectivas de expertos en el campo, lo que enriquecerá significativamente el análisis.

En resumen, esta investigación se basará en una sólida base de datos cualitativos recopilados a partir de fuentes bibliográficas, publicaciones en la web y entrevistas con especialistas. El enfoque descriptivo nos permitirá proporcionar una visión completa y detallada del perfil criminal de los hackers, mientras que el enfoque cualitativo ayudará a comprender mejor las motivaciones, estrategias y tendencias detrás de sus actividades delictivas. Este enfoque integral permitirá abordar de manera efectiva la complejidad de este tema en constante evolución.

RESULTADOS

Existe una convención, el Black Hat, que es la conferencia de seguridad que reúne a cientos de hackers de todo el mundo, fue la demostración de la existencia de vulnerabilidades en objetos que son impensados para el usuario corriente. Sin embargo, una de las curiosidades es la naturaleza misma de los presentadores en Black Hat, gurús de seguridad que se refieren a sí mismos, y con orgullo, como “hackers”. En este punto es necesario hacer una pequeña aclaración: a diferencia de los cibercriminales, los hackers no necesariamente se dedican a robar el dinero de las personas. Para entender cuáles son las motivaciones de estos genios de la informática, Thycotic, una reconocida compañía de seguridad, realizó una encuesta a más de 100 hackers que asistieron a Black Hat, con el objetivo de conocer qué los impulsa a hackear ciertos sistemas y cuáles son estrategias de preferencia.

La encuesta arrojó varios resultados llamativos. El 86 % de los hackers está convencido de que nunca serán castigados por sus acciones y no asumen responsabilidad alguna sobre las consecuencias. Al parecer, la impunidad es la primera llamada a la acción en el cibercrimen.

El 40 % de los hackers afirma que su objetivo primario en un ataque serían los contratistas de la compañía.

Otro punto interesante es a quién elegirían los hackers, dentro del personal de una compañía, como objetivo de un ataque a fin de infiltrarse en un sistema. El 40 % de los encuestados afirma que su primera opción serían los contratistas de la empresa, ya que éstos tienen acceso a las redes corporativas y no están completamente regulados por las políticas de seguridad.

Curiosamente, los administradores de IT (por sus siglas en inglés “Information Technology”) son la segunda opción. A pesar de

que el personal de IT, al menos en la teoría, debería estar completamente preparado para manejar un ataque de este tipo, el 30 % de los hackers aseguró que dirigiría sus ataques a ellos para ingresar a la red de la compañía.

Los resultados de la encuesta nos sorprendieron, ya que la lista de Thycotic no incluía al personal de recursos humanos, que tradicionalmente son marcados como el objetivo potencialmente más vulnerable a un ataque.

Por otra parte, la encuesta también reveló que el 51 % de los hackers suele realizar ataques por la mera diversión de hacerlo. Sin embargo, el 30 % de los encuestados asegura que nunca infringe sus principios éticos.

Finalmente, el 88 % de los hackers asegura que, a pesar de contar con grandes capacidades y conocimientos en computación, ni siquiera ellos están exentos de convertirse en víctimas de un ataque o de un robo masivo de datos, perpetrado por otros hackers.

DISCUSIÓN

Del análisis de los datos obtenidos, el perfil de los hackers indica que, en su mayoría son de sexo masculino (aproximadamente un 90 %). En un 80 % son menores de 30 años. La mayoría tienen una inteligencia lógico-matemática mayor al promedio de la población y son de contextos socio económicos de clase media alta. No son del tipo de delincuentes que actúan por necesidad económica. El principal móvil de la mayoría de ellos es la autosuperación y la búsqueda de "nuevas sensaciones", diversión y adrenalina por delinquir, además de probarse a sí mismos ser capaces y ser mejores que grandes empresas. Son personas que aun pudiendo utilizar sus habilidades para hacer un bien y sin necesidades socio económicas a cubrir, deciden delinquir. En palabras textuales "Analizo personas, busco vulnerabilidades y los manipulo". Es decir, son personas que utilizan la ingeniería social, es decir, a gran escala, son personas con rasgos narcisistas.[15,16]

Para realizar el análisis psicológico me base en el modelo PEN de personalidad de Eysenck.[17] Este modelo se basa en la idea de que la personalidad puede ser entendida en términos de tres factores fundamentales: psicoticismo (P), extraversión (E) y neuroticismo (N). El psicoticismo se refiere a la tendencia de una persona a mostrar rasgos como la agresión, la impulsividad, la insensibilidad emocional y la falta de empatía. Las personas con altos niveles de psicoticismo tienden a ser más atrevidas, dominantes y propensas a comportamientos antisociales. Pueden mostrar una menor capacidad para entender las emociones de los demás y pueden carecer de empatía hacia los demás. El factor de extraversión (E) se relaciona con la sociabilidad, la búsqueda de estimulación y la energía. Las personas extrovertidas tienden a ser enérgicas, sociables, habladoras y buscan la interacción social. Disfrutan estar rodeadas de otras personas y pueden ser más extrovertidas en situaciones sociales. Los extrovertidos suelen buscar estímulos externos y pueden disfrutar de actividades que implican interacción con otras personas. El neuroticismo (N) es otro factor importante en el modelo PEN. Se refiere a la tendencia de experimentar emociones negativas, como la ansiedad, la inestabilidad emocional y la tendencia a preocuparse. Las personas con altos niveles de neuroticismo suelen ser más propensas a experimentar estrés y emociones negativas en situaciones desafiantes. Pueden ser más sensibles a los cambios en su entorno y pueden tener dificultades para manejar el estrés. Es importante tener en cuenta que estos factores no son absolutos ni determinantes, sino que representan tendencias generales en la personalidad. Cada individuo es único y puede mostrar diferentes niveles de cada factor en diferentes momentos y situaciones.

Uno de los rasgos característicos del hacker es la frialdad y la ausencia de nerviosismo, la capacidad de mantener el control pase lo que pase. Son personas que pueden tolerar niveles de estrés, tensión, ansiedad elevado. Aplicando el modelo PEN de personalidad, puntuarían muy bajo en neuroticismo, son personas con mucha estabilidad emocional. Son personas que no se ponen nerviosas, no manifiestan ansiedad ni nervios.

Por otro lado, ser hacker requiere pasar mucho tiempo solos, analizando, estudiando. Son personas solitarias, menos sociables que el resto. Personas fuertemente introvertidas, analíticas, tranquilas, previsoras, planificadoras. Muchos hackers se encuentran dentro del espectro autista. Con alto nivel de percepción del detalle y de sistematización. Otros de los rasgos comunes entre el autismo y los hackers son los rasgos obsesivos-compulsivos y la capacidad alta de concentración.

Para finalizar con los conceptos PEN de la personalidad, son personas con psicoticismos altos, suelen tener dificultades para integrarse y adaptarse en sociedad. les cuesta integrar las normas sociales, son menos sensibles a los castigos. Tienen menos conciencia social. Son propensos a comportamientos delictivos. Personas intelectuales, solitarias, independientes, vistas socialmente como "raras".

CONCLUSIONES

Otra conclusión a la que puedo llegar después de realizada esta investigación es que al ser la tecnología algo en constante desarrollo en el mundo, y en particular en nuestro país, no se ha podido encontrar un equilibrio para adaptar los ordenamientos jurídicos a su vorágine, su cambio constante. La legislación argentina no está actualizada, las leyes que abordan la ciberdelincuencia se modificaron hace más de diez años, algo que queda muy atrasado con respecto a los cambios permanentes en el cibercrimen.

Una medida de prevención sería implementar un sistema cibernético mundial con el propósito de supervisar y regular de manera más efectiva las actividades en línea, identificando patrones y comportamientos sospechosos mediante algoritmos avanzados creados por expertos. Además, la creación de una base de datos global, permanentemente actualizada y compartida entre entidades gubernamentales y fuerzas del orden, podría mejorar la capacidad de seguimiento y persecución de aquellos que se dedican a actividades delictivas en línea. Como otra medida se podrían establecer mecanismos de autenticación más rigurosos para mitigar el problema del anonimato, requiriendo identificación verificable en diversas interacciones en línea. Asimismo, la cooperación internacional sería fundamental, permitiendo la rápida transferencia de información y la ejecución de acciones coordinadas para abordar delitos cibernéticos que trascienden fronteras. Para fortalecer este sistema, sería crucial invertir en tecnologías de seguridad de vanguardia y en la capacitación continua de profesionales dedicados a la ciberseguridad. La concienciación pública sobre las amenazas cibernéticas y la promoción de prácticas seguras en línea también deberían ser componentes integrales de cualquier

estrategia global para combatir la actividad delictiva digital.

FINANCIACIÓN
Ninguna.

CONFLICTO DE INTERESES
Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA
Conceptualización: Rocío Magalí Méndez, María Inés Lanza.
Curación de datos: Rocío Magalí Méndez, María Inés Lanza.
Análisis formal: Rocío Magalí Méndez, María Inés Lanza.
Investigación: Rocío Magalí Méndez, María Inés Lanza.
Metodología: Rocío Magalí Méndez, María Inés Lanza.
Administración del proyecto: Rocío Magalí Méndez, María Inés Lanza.
Recursos: Rocío Magalí Méndez, María Inés Lanza.
Software: Rocío Magalí Méndez, María Inés Lanza.
Supervisión: Rocío Magalí Méndez, María Inés Lanza.
Validación: Rocío Magalí Méndez, María Inés Lanza.
Visualización: Rocío Magalí Méndez, María Inés Lanza.
Redacción – borrador original: Rocío Magalí Méndez, María Inés Lanza.
Redacción – revisión y edición: Rocío Magalí Méndez, María Inés Lanza.

REFERENCIAS BIBLIOGRÁFICAS
1. Argentina.gob.ar. Qué es el ciberdelito. 2023. Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

2. AALCC. Estadísticas 2021: informe sobre consultas en materia de delitos configurables a través de internet. 2021. Disponible en: https://www.cibercrimen.org.ar/2021/12/28/estadisticas-2021/

3. Argentina.gob.ar. Caracterización de la criminalidad organizada. 2022. Disponible en: https://www.argentina.gob.ar/seguridad/abordaje-crimen-organizado/criminalidad-organizada

4. Di Iorio AH, Castellote MA, et al. El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense. Mar del Plata: Grupo de Investigación en Sistemas Operativos e Informática Forense, Universidad FASTA; 2016.

5. Campus Ciberseguridad. Tipos de hackers. Disponible en: https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackers

6. Diario Perfil. Un hackeo en el Ministerio Público Fiscal generó preocupación en el poder judicial. 2021. Disponible en: https://www.perfil.com/noticias/politica/hackeo-ministerio-publico-fiscal-genero-preocupacion-poderjudicial.phtml

7. Clarín. El CONICET víctima de ciberdelincuentes: roban datos y piden dinero para devolverlos. 2022. Disponible en: https://www.clarin.com/tecnologia/conicet-victima-ciberdelincuentes-roban-datos-piden-dinero-devolverlos_0_LFRRFW39jx.html

8. Clarín. El Senado de la Nación sufrió un ciberataque de tipo ransomware. 2021. Disponible en: https://www.clarin.com/tecnologia/senado-nacion-sufrio-ciberataque-ransomware-secuestrandatos-publicos_0_13uPrKQNd.html

9. La Nación. Migraciones: cómo fue el ataque del ransomware Netwalker y qué datos revela. 2020. Disponible en: https://www.lanacion.com.ar/tecnologia/migraciones-como-fue-ataque-del-ransomware-netwalkernid2446451/

10. Correo Argentino. Alerta: usan el nombre de Correo Argentino para una nueva estafa virtual. 2021. Disponible en: https://www.correoargentino.com.ar/alerta-usan-el-nombre-de-correo-argentino-para-una-nuevaestafa-virtual

11. Infobae. Hackearon el sistema de PAMI: qué pasará con los turnos y con las recetas para medicamentos. 2023. Disponible en: https://www.infobae.com/economia/2023/08/02/hackearon-el-sistema-de-pami-que-pasara-con-los-turnos-y-con-las-recetas-para-medicamentos/

12. Comercio y Justicia. En 2023, la inversión tecnológica será prioridad para el Poder Judicial de Córdoba. 2022. Disponible en: https://comercioyjusticia.info/suplementoaniversario/2022/10/31/en-2023-la-inversion-tecnologica-sera-prioridad-para-el-

poder-judicial-de-cordoba/

13. La Voz. Por el hackeo, el TSJ determinaría que el martes sea feriado judicial. 2022. Disponible en: https://www.lavoz.com.ar/sucesos/por-el-hackeo-el-tsj-determinaria-que-el-martes-sea-feriado-judicial/

14. La Voz. Colegio de Abogados, preocupado por ciberataque a la Justicia, pide explicaciones al Tribunal Superior. 2022. Disponible en: https://www.lavoz.com.ar/sucesos/colegio-de-abogados-preocupado-por-ciberataque-a-la-justicia-y-pide-explicaciones-al-tribunal-superior/

15. Kaspersky LATAM. Cuáles son las principales motivaciones de los hackers. Disponible en: https://latam.kaspersky.com/blog/cuales-son-las-principales-motivaciones-de-los-hackers/3853/

16. United Nations Office on Drugs and Crime (UNODC). Crimen organizado transnacional. 2020. Disponible en: https://www.unodc.org/ropan/es/organizedcrime.html

17. Mentes Abiertas Psicología. El modelo PEN de Eysenck: comprendiendo la personalidad desde una perspectiva científica. Disponible en: https://www.mentesabiertaspsicologia.com/blog-psicologia/blog-psicologia/el-modelo-pen-de-eysenck-comprendiendo-la-personalidad-desde-una-perspectiva-cientifica