TECNOCIENCIA CHIHUAHUA
Revista de ciencia y tecnología
ISSN-e: 2683-3360

UACH
UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA

Artículo de Revisión

Ataques a celulares a través del uso de aplicaciones móviles: Una revisión narrativa

Attacks on Cell Phones Through the Use of Mobile Applications: A Narrative Review

Aldair Olguin-Romero*[1], Julia Arana-Llanes[1]

[1] Licenciatura en Ingeniería de Software | Universidad Autónoma del Estado de Hidalgo, Escuela Superior de Tlahuelilpan. Ex Hacienda de San Servando, Av. Universidad s/n Centro, Tlahuelilpan, Hgo., México.

*Correspondencia: Correo electrónico: ol434947@uaeh.edu.mx (Aldair Olguin-Romero)
DOI: https://doi.org/10.54167/tch.v18i3.1584
Recibido: 25 de junio de 2024; **Aceptado**: 17 de octubre de 2024
Publicado por la Universidad Autónoma de Chihuahua, a través de la Dirección de Investigación y Posgrado.

Resumen

Algunas aplicaciones móviles se pueden utilizar para ataques a teléfonos móviles. Estos programas maliciosos pueden robar la información personal, como contraseñas e información financiera, o instalar *malware* en su dispositivo. Los ataques se pueden llevar a cabo mediante la descarga de software fraudulento, mensajes de texto y correos electrónicos con enlaces maliciosos y comprometiendo el sistema operativo. Los usuarios deben tener cuidado al descargar aplicaciones de fuentes desconocidas, mantener sus dispositivos actualizados y utilizar medidas de seguridad como instalar aplicaciones desde las apps store oficiales o proveedores confiables, revisar y ajustar los permisos de las aplicaciones para proteger sus dispositivos de amenazas. Estudios sobre ciberseguridad indican que, si bien el número de intrusiones a teléfonos móviles han aumentado, inversamente dichos ataques se han sofisticado y su capacidad destructiva o de afectación se ha incrementado.

***Palabras clave*: aplicaciones, dispositivos, información, seguridad, amenazas**

Abstract

Some mobile apps can be used for attacks on mobile phones. These malicious programs can steal personal information, such as passwords and financial information, or install malware on your device. Attacks can be carried out by downloading fraudulent software, text messages, and emails with malicious links, and compromising the operating system. Users should be careful when downloading apps from unknown sources, keep their devices up to date, and use security measures such as installing apps from official app stores or trusted providers, reviewing and adjusting app permissions to protect their devices from threats. Studies on cybersecurity indicate that, although the number of intrusions to mobile phones has decreased, conversely these attacks have become more sophisticated and their destructive or affecting capacity has increased.

***Keywords*: applications, devices, information, security, threats**

1. Introducción

Los móviles son dispositivos electrónicos versátiles que van más allá de las llamadas, permitiendo fotografías, mensajería, juegos, lectura y diseño. Equipados con sistemas operativos evolucionados, son comparables en potencia a los ordenadores y portátiles (Morte, 2019).

Sin embargo, es extraordinario el hecho de que sólo ha pasado una década desde que se comenzó a prestar atención al uso y abuso de los teléfonos inteligentes, y sólo en tiempos recientes se ha empezado a prestar atención a los problemas que el uso excesivo de los teléfonos móviles puede causar en nuestra vida diaria, así como en el desempeño laboral, social y familiar, afectando las prácticas sociales básicas, con los otros individuos (Ceberio, 2019).

Las intrusiones de tipo *hackeo* a los móviles, se encuentran entre los mayores peligros de seguridad. Esto sucede cuando la información de suscripción a las cuentas de las aplicaciones contenidas se ve comprometida o robada, lo cual implica una gran pérdida de información debido a que estos dispositivos son el lugar desde donde se gestiona y almacena información de casi cualquier propósito, como acceder a cuentas bancarias, realizar pagos, enviar mensajes y más. Si un intruso logra acceder al dispositivo, puede suplantar la identidad del usuario, infectar a otros contactos y robar datos (Jiménez, 2024).

Para entender la gravedad de este problema, es crucial examinar tanto las características de las aplicaciones como los métodos utilizados por los atacantes para poner en riesgo la información de los usuarios. Por ello, este documento se ha basado en analizar investigaciones recientes, los cuales han revelado un aumento en la cantidad y complejidad de estos ataques, lo que subraya la importancia de abordar este tema con seriedad. En este contexto, es fundamental explorar las acciones de protección y prevención que los usuarios pueden adoptar para salvaguardarse de estos ataques.

Con la creciente facilidad de uso de los dispositivos móviles, tanto las organizaciones como los usuarios están cada vez más inclinados a comprar y utilizar estos dispositivos en lugar de computadoras de escritorio. Asimismo, el acceso inalámbrico a Internet se vuelve más común, lo que provoca que se vuelvan más vulnerables a ataques.

Hoy en día los criminales cibernéticos han demostrado contar con habilidades suficientes para atacar cámaras de vigilancia, monitores para bebés y dispositivos médicos implantados, entre otros, lo que los convierte en una seria amenaza a la seguridad en cualquier ámbito. Se proyecta que para 2025, más de 75 mil millones de dispositivos estarán conectadas a Internet (IoT) *Internet of things* entre las que se podrían incluir cámaras, televisores inteligentes, monitores de salud y muchos otros dispositivos similares según el informe sin fecha de International Business Machines Corporation (IBM, s.f.).

El *malware (Software malicioso, Adware: publicidad intrusiva)* móvil va en aumento, ya que los atacantes han pasado a dedicar sus esfuerzos a los smartphones y tabletas. Para lograr evitar o mitigar dichas amenazas es necesario reconocer los riesgos existentes y la forma de los ataques, así como siempre seguir los consejos y buenas prácticas de los especialistas (Kaspersky, s.f.).

Las vulnerabilidades más frecuentes en los dispositivos móviles con sistema Android, son ocasionadas por la descarga de aplicaciones libres desde fuentes no seguras, en lugar de usar la tienda oficial Play Store de Google, es necesario que los usuarios tengan conciencia de hasta qué grado vulneran su información sensible al instalar estas aplicaciones, ya que pueden tener acceso a navegadores, galería, mensajes, llamadas, ubicación, entre otras. Las aplicaciones cuando se instalan solicitan una serie de permisos y entre ellos se encuentran los que facilitan el ingreso a las funciones mencionadas, es donde se ven expuestos y vulnerables a cualquier tipo de ataque informático o de uso no autorizado (ASPRILLA, 2021).

2. Metodología

Se hizo una revisión metodológica de textos especializados en los diferentes métodos de ataques a dispositivos móviles, dichos textos han sido basados de análisis de datos obtenidos por sistemas de antivirus como Kaspersky, así como las medidas más efectivas para prevenir y mitigar estos ataques.

Es importante conocer e identificar los métodos de ataque y sus consecuencias, ya que los atacantes emplean una diversidad de técnicas para ingresar en nuestros dispositivos mediante aplicaciones móviles, incluidos el *phishing*, el *malware* y los puntos débiles del sistema. Por medio de estudios de casos reales, se han examinado las consecuencias devastadoras para los usuarios y las empresas.

3. Población de estudio

Según Kaspersky, en información citada por Kivva (2023), los dispositivos móviles que utilizan su antivirus están expuestos a la detección de tráfico malicioso durante la navegación en internet, cabe destacar que este estudio consideró a toda la población en edad de poseer y con capacidad de operar teléfonos celulares o dispositivos móviles, según (INEGI, 2023) en México para el año 2023, 97.2 millones de personas utilizaban dispositivos móviles, lo que implica rangos de edad de apartir de 6 años y superando los 64 años, sin distinción de género, raza o posición social, entre otros. Este tráfico puede originarse en diversas aplicaciones móviles, que abarcan desde redes sociales y mensajería hasta banca móvil y servicios de salud. La proliferación de aplicaciones en las plataformas móviles genera un entorno en el que cualquier dispositivo puede ser vulnerable al tráfico

malicioso, lo que resalta la importancia de implementar soluciones de seguridad efectivas para identificar y mitigar estos riesgos en tiempo real.

4. Revisión de literatura para la identificación de ciberataques

Como usuario, es de suma importancia conocer el crecimiento y existencia de los ataques cibernéticos a teléfonos móviles y con esto evitar seguir cayendo en este tipo de estafas e intrusiones, así como conocer el su impacto y posibles consecuencias (Medina, 2024), debido a que pueden provocar perdidas de información o ataques de robo de identidad. Según (Garcia Garcia, 2020) dice que los problemas han incrementado debido a la evolución y el impacto del uso de los smartphones en la sociedad actual, ya que dicha evolución sucede basada en las necesidades de los usuarios y las posibilidades de procesos a realizar por dichos dispositivos.

Por otra parte, es conocido que los usuarios solo requieren cubrir la necesidad del uso de este tipo de dispositivos, sin tomar en cuenta los riegos que esto puede conllevar tal y como no los explica (Córdoba Cadena, s.f.), donde analiza las vulnerabilidades a las que se exponen los usuarios durante el uso de dispositivos móviles, poniendo en riesgo información de los mismos y teniendo como principal ataque el malware como el riesgo más común detectado, también la existencia de conexiones inseguras y phishing. Dentro de (Vargas Santana, 2023) se destaca que, los dispositivos móviles se han convertido en gran necesidad para las personas en ámbitos laborales y personales. Así mismo se menciona que el sistema operativo Android se ha convertido en el más utilizado al nivel mundial, y por tal motivo, crece de manera rápida la generación y uso de millones de aplicaciones disponibles en la Play Store, lo que provoca que los usuarios realicen varias descargas sin conocer los riegos que estas apps pueden traer.

Finalmente, (Vargas Santana, 2023) destaca que ninguna red es segura al igual que, (Kaspersky, s.f.) menciona, que las amenazas de seguridad móvil están en aumento, siendo las principales amenazas la filtración de datos, redes Wi-Fi no seguras, suplantación de redes, ataques de phishing, ataques de spyware, criptografía quebrada y mala gestión de sesiones. Lo anterior se ha debido a la gran cantidad de datos que almacenan y la vulnerabilidad que esto representa, destacando como un caso notable a Pegasus, el ataque a WhatsApp en 2019, y el malware Joker en Android.

Por otro lado, debido a que los teléfonos móviles se han vuelto cruciales y cada vez más utilizados en las actividades diarias, ha ocasionado que tengan que tomarse algunas medidas de seguridad para la protección de dichos dispositivos, ya que (Lab, 2024) reporta un aumento del 50% en amenazas móviles, alcanzando casi 33.8 millones de ataques, dejando al adware como la amenaza más común con un 40.8%.

Finalmente, es notable señalar que las amenazas a menudo se distribuyen a través de aplicaciones maliciosas en tiendas oficiales y no oficiales, por ello (Kaspersky, s.f.) recomienda descargar aplicaciones solo de tiendas oficiales, revisar permisos, usar soluciones de seguridad confiables y mantener las aplicaciones actualizadas.

5. Clasificación de los tipos de amenazas

A partir de la información recopilada mediante la literatura para este estudio, es posible identificar los ataques preferidos contra teléfonos móviles por los ciberdelincuentes**,** los cuales son descritos a continuación.

1. *Malware*:

    - *Troyanos*: Aplicaciones que parecen legítimas pero que contienen software malintencionado que puede extraer información, enviar mensajes SMS premium, o tomar control del dispositivo.

    - *Spyware*[1]: Software malicioso diseñado para obtener datos de las actividades del usuario, como ubicaciones, mensajes y contraseñas.

    - *Adware*: Aplicaciones que muestran anuncios de manera excesiva y obtienen información del usuario para mostrar publicidad dirigida.

2. *Phishing*[2]

    - Aplicaciones falsas: Imitan aplicaciones legítimas con el propósito de confundir a los que usen la aplicación y obtener sus Credenciales de acceso, información bancaria u otros datos sensibles.

    - Links maliciosos: Enlaces incluidos en aplicaciones que te redireccionan a sitios de internet fraudulentos diseñados para adquirir información personal.

3. *Ransomware*:

    - Aplicaciones que bloquean el acceso al teléfono móvil o cifran la información del usuario, exigiendo un rescate para devolver el acceso.

4. *Exploits*[3]:

[1] *Spyware: Es una forma de software perjudicial que se instala en un dispositivo sin el permiso del usuario para recoger información de manera clandestina, a menudo con la intención de espiar o robar datos.*
[2] *Phishing: El phishing es una estrategia engañosa empleada por delincuentes cibernéticos para inducir a los usuarios a revelar información personal confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios.*
[3] *Exploit: Se refiere a un programa informático o conjunto de instrucciones utilizadas por personas malintencionadas para aprovechar debilidades en sistemas o software, permitiéndoles llevar a cabo acciones no autorizadas o dañinas.*

- Vulnerabilidades de día cero: Ataques que aprovechan vulnerabilidades desconocidas en el software para obtener acceso no autorizado o control del dispositivo.

- Rooting/Jailbreaking: Técnicas utilizadas para obtener acceso administrativo completo al sistema operativo del dispositivo, permitiendo la instalación de aplicaciones maliciosas que pueden eludir las medidas de seguridad estándar.

5. Ataques de hombre en el medio (MitM):

    - Aplicaciones que interceptan y manipulan las comunicaciones entre el móvil y los servidores, pudiendo robar información o modificar datos sin que la persona lo sepa.

6. Ataques de suplantación (*Spoofing*):

    - Suplantación de identidad (Spoofing de aplicaciones): Aplicaciones que se hacen pasar por otras para engañar a los usuarios y robar información.

7. *Backdoors*[4]:

    - Aplicaciones que instalan puertas traseras en el equipo, permitiendo a los intrusos entrar al dispositivo y sus datos sin el conocimiento del usuario.

8. Ataques vía librerías y *SDKs*[5]:

    - Muchas aplicaciones utilizan librerías de terceros y *SDKs* que cuentan con fallos o código malicioso que compromete la seguridad del dispositivo.

9. Ataques por permisos excesivos:

- Aplicaciones que solicitan más permisos de los requeridos para poder llevar a cabo su ejecución, y luego utilizan estos permisos para obtener datos sensibles u operaciones del dispositivo.

[4] *Backdoor: es una entrada secreta en un sistema informático, permitiendo el acceso sin seguir los procedimientos normales de autenticación, lo cual puede ser utilizado tanto para fines legítimos como para actividades ilegales.*

[5] *SDKs: Kits de Desarrollo de Software.*

6. Datos e interpretación

El aumento en la incidencia de ciberataques es un fenómeno alarmante que se ha visto impulsado, en gran parte, por la amplia disponibilidad de aplicaciones en tiendas oficiales y no oficiales. Esta accesibilidad permite que los usuarios descarguen programas sin ser plenamente conscientes de los riesgos que pueden conllevar. A medida que los dispositivos móviles continúan evolucionando y sus capacidades se expanden, la cantidad de datos sensibles almacenados, se convierten en objetivos atractivos para los ciberdelincuentes. En este contexto de creciente vulnerabilidad. Por lo anterior es crucial implementar medidas de seguridad efectivas y educar a los usuarios sobre los peligros asociados con el uso de aplicaciones móviles. A continuación, se presentarán datos relevantes e interpretaciones que arrojarán luz sobre esta problemática y su impacto en la seguridad digital.

En 2021, los productos y tecnologías móviles de Kaspersky detectaron:

- 3.464.756 archivos de instalación con intenciones maliciosas;
- 97.661 nuevas variantes de software malicioso destinado a robar información bancaria de dispositivos móviles.;
- 17.372 nuevos troyanos extorsionadores (*ransomware*) para dispositivos móviles.

Por otra parte, en el año 2022, se registraron 22,255,956, dato que en 2023 pasó a registrar 33,790,599 casos, documentándose así un incremento del 52% en la incidencia (Lab, 2024).

En el primer trimestre de 2023 con información de Kaspersky Security:

- Se reprimieron 4 948 522 ataques con *software* [6] móvil malicioso, *adware* o no deseado.
- Por otra parte, el *adware* o publicidad fue el peligro más usual para los móviles, siendo un 34,8% de los riesgos detectados.
- También, fueron identificados 307,529 paquetes maliciosos, de los cuales
    - 57,601 eran troyanos bancarios móviles;
    - 1,767 eran troyanos extorsionadores móviles.

[6] *Software: Programa informático*

A pesar de que los intentos de intrusión a dispositivos celulares mediante malware, adware o software no deseado persisten, Kaspersky reporta que logró evitar más de 4,9 millones de ataques (Kivva, 2023).

Al mismo tiempo, se identificó que los tipos de ataques pueden variar en su naturaleza y alcance, incluyendo malware que se propaga con apps falsas o comprometidas, como lo es el phishing que solicita a los usuarios acceder a un correo, enlace o sitio, con el fin de que revelen información personal. Por otra parte, también existen los ataques de ingeniería social que manipulan a los usuarios para llevar a cabo acciones no deseadas como revelación de datos personales como contraseñas, números de tarjetas de crédito entre otros.

Por otra parte, los atacantes a menudo buscan explotar vulnerabilidades en el sistema o en las propias aplicaciones para obtener acceso no autorizado al equipo o a los datos almacenados en él.

Los usuarios afectados por estos atacantes suelen enfrentar una serie de consecuencias negativas, que van desde el robo de datos personales y financieros hasta la usurpación de identidad.

Por esta razón detectar y mitigar estos ataques puede ser desafiante debido a la rápida evolución de las técnicas utilizadas por los atacantes y el elevado número de aplicaciones disponibles en las plataformas de aplicaciones.

Por otra parte, la conciencia y la educación del usuario son fundamentales para contribuir a evitar estos ataques. Los usuarios deben ser conscientes de los peligros vinculados al descargar aplicaciones de fuentes poco fiables y deben estar capacitados para reconocer indicadores de alerta de posibles ataques, como solicitudes de privilegios exagerados o comportamiento inusual.

Además, la innovación en seguridad debe ser constante debido a la evolución de los peligros, y así lograr que las mejoras en seguridad también avancen. Es crucial seguir innovando en métodos de identificación de amenazas, examinar el comportamiento y herramientas de seguridad móvil para estar al tanto de los últimos riesgos.

Es fundamental que los usuarios solo descarguen aplicaciones de tiendas autorizadas, verifiquen las revisiones y los permisos requeridos por las mismas y actualicen sus aplicaciones para protegerse contra estas amenazas.

Dentro de la Fig. 1, es posible observar los principales ataques en el lapso reportado por Kivva (2023), así como el tipo de virus o ataques principales.

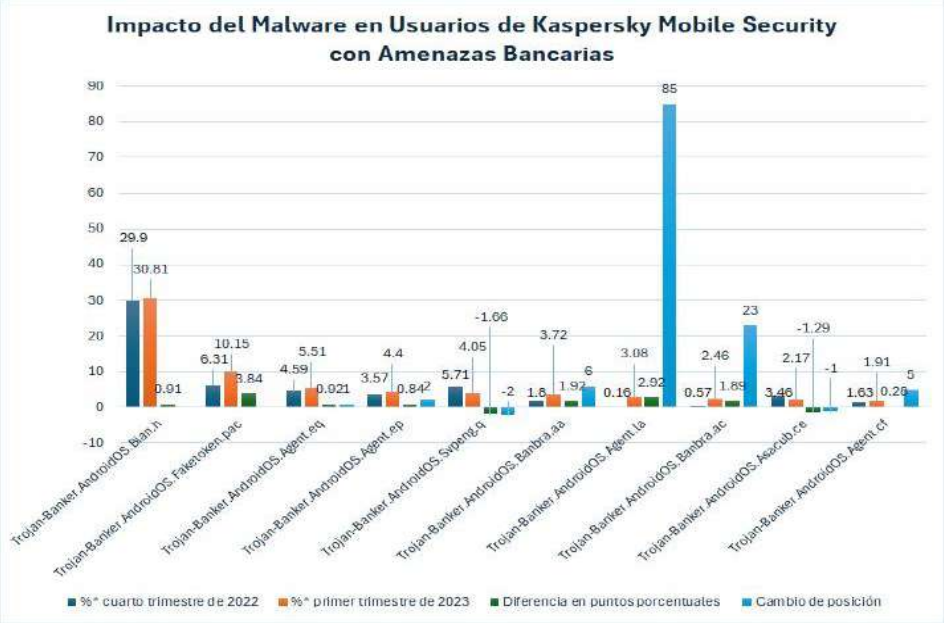

Figura 1. Impacto del malware en los usuarios de Kaspersky Mobile Security con amenazas bancarias. Tomado de Securelist (Kirva, 2023).
Figure 1. Impact of malware on Kaspersky Mobile Security users with banking threats. Taken from Securelist (Kirva, 2023).

7. Conclusiones y recomendaciones

Los ataques a dispositivos móviles mediante aplicaciones son una grave amenaza en el contexto de la ciberseguridad. La dependencia creciente de los dispositivos móviles en nuestra vida cotidiana, junto con la sofisticación de las recurrentes amenazas, han creado un entorno vulnerable para los ataques y extracción de datos de los usuarios de celulares.

La prevención contra estos ataques necesita una perspectiva integral que involucre a usuarios, desarrolladores, empresas y reguladores trabajando juntos. Los usuarios deben ser educados sobre las amenazas vinculadas con la utilización de aplicaciones móviles y practicar acciones de protección digital, como descargar aplicaciones solo de sitios oficiales y mantener actualizados sus dispositivos.

Además, la colaboración entre la industria tecnológica y los reguladores gubernamentales es crucial para abordar los fallos de seguridad y promover medidas de protección adecuadas en el ecosistema móvil.

En definitiva, defenderse de amenazas por aplicaciones móviles es un esfuerzo continuo que requiere vigilancia y cooperación en los distintos niveles. Únicamente teniendo una mezcla de concienciación, educación y acción proactiva podemos mitigar eficazmente esta creciente amenaza. Por lo anterior se ha definido un grupo de recomendaciones que se muestran en la Figura 1 lo cual ayudara a reducir el problema de ciber ataques a dispositivos móviles.

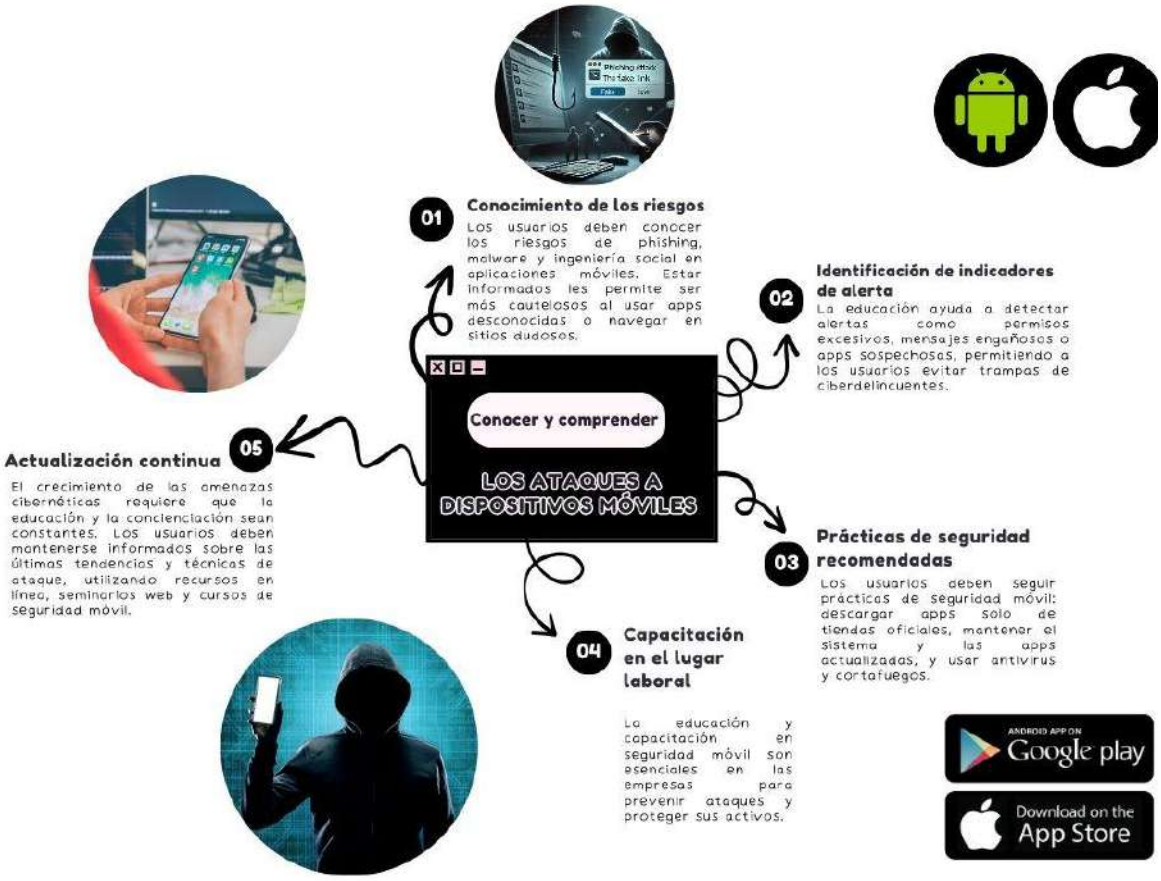

Figura 2. Prevención de ataques a dispositivos móviles.
Figure 2. Preventing mobile device attacks.

Implementando estas recomendaciones, se pueden fortalecer la defensa contra los ataques a dispositivos móviles y así asegurar datos personales y profesionales.

Conflicto de interés

El autor declara que no existe ningún conflicto de interés relacionado con la investigación y publicación de este artículo sobre los ataques a teléfonos móviles a través del uso de aplicaciones móviles.

Referencias

Lab, A. K. (2024). Los ataques a dispositivos móviles aumentaron más del 50% en 2023. https://goo.su/3TVUdVF

Ceberio, D. M. (2019). ADICCIÓN Y USO DEL TELÉFONO CELULAR. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2077-21612019000200001

Córdoba Cadena, J. E. (s.f.). Vulnerabilidad En Dispositivos Móviles. https://repository.ucc.edu.co/entities/publication/bd16b591-9260-4579-bf63-14e77e51b7c5

ASPRILLA, O. E. (2021). ANÁLISIS DE RIESGO DE SEGURIDAD EN LOS DISPOSITIVOS MÓVILES. Universidad Nacional Abierta y a Distancia UNAD: https://goo.su/08RGfy

Garcia Garcia, M. (01 de 2020). Seguridad en dispositivos móviles: Análisis de riesgos, de vulnerabilidades y auditorías de dispositivos. http://hdl.handle.net/10609/107326

IBM. (s.f.). ¿Qué es la seguridad móvil? https://www.ibm.com/mx-es/topics/mobile-security

INEGI. (2023). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares. https://goo.su/EUWE

Jiménez, J. (5 de 1 de 2024). RZ. https://www.redeszone.net/tutoriales/seguridad/que-hacer-hackeado-movil/

Kaspersky. (s.f.). Amenazas a la seguridad móvil para Android. https://www.kaspersky.es/resource-center/threats/mobile

Kivva, A. (2023). Evolución de las amenazas informáticas en el primer trimestre de 2023. Estadísticas de amenazas móviles. Kaspersky. https://securelist.lat/it-threat-evolution-q1-2023-mobile-statistics/97916/

Medina, H. B. (2024). Análisis de vulnerabilidades en dispositivos móviles con sistema operativo Android. https://caoba.sanmateo.edu.co/ojs/index.php/sistemas/article/view/192

Morte, D. G. (2019). Estudio de dispositivos móviles, vulnerabilidades y auditoría de seguridad de aplicaciones móviles. https://goo.su/IWkd

Vargas Santana, L. L. (2023). Análisis de vulnerabilidades críticas del sistema operativo móvil Android mediante Pentesting. https://repositorio.puce.edu.ec/handle/123456789/38132

2024 TECNOCIENCIA CHIHUAHUA.

Esta obra está bajo la Licencia Creative Commons Atribución No Comercial 4.0 Internacional.

https://creativecommons.org/licenses/by-nc/4.0/