



ספטמבר 2024

אלול תשפ"ד

המלצות להתנהלות הציבור בשימוש באפליקציות תיירות

רקע

שוק התיירות המקוון הפך ברבות השנים לענף של מיליארדי דולרים וחולל מהפכה מוחלטת באופן שבו אנו מתכננים, מזמינים וחווים נסיעות וחופשות. מהפכה שרחוקה מלהסתיים, כפי שהוכח לאחרונה בהטמעה של שירותי בינה מלאכותית (AI) בתחום התיירות¹ ובהתפתחות המשגשגת של אפליקציות להזמנת נסיעות.²

בעידן הדיגיטלי, אפליקציות להזמנת נסיעות הפכו לכלי חיוני עבור אלו המבקשים לטייל. אפליקציות אלו מציעות נוחות וחווית הזמנה, אך הן גם מעלות חששות לגבי פגיעה בפרטיות המשתמשים, בשל הכמות העצומה של המידע האישי שהן אוספות ומבקשות במהלך תהליך ההזמנה והשימוש בשירות.

נוסעים המשתמשים ביישומים מקוונים לאורך כל תהליכי התכנון וההזמנה מתמודדים עם **בקשות רבות למידע אישי**. בקשות אלו מגיעות ממספר רב של ספקי שירותים, כגון חברות תעופה, בתי מלון, סוכנויות נסיעות, מפתחי אפליקציות תיירות למכשיר הנייד, מפתחי טכנולוגיות ושירותים מבוססי מיקום (LBS),³ פלטפורמות לסקירות תיירות מקוונות, אתרי רשתות חברתיות ואחרים. חלק מהספקים הללו הם מקומיים ומותאמים ליעד הנסיעה,⁴ וחלקם מקושרים זה לזה (למשל, בתי מלון בשיתוף עם סוכנויות השכרת רכב ומפעילי שירותי תרבות) ולכן עשויים לחלוק חלק מסוים מנתוני הלקוחות. כתוצאה מכך, המורכבות סביב **השיתוף של נתוני ספקי נסיעות מקוונים שונים** עלולה להגביר את הפגיעה בפרטיות מעבר לשימוש הרגיל באינטראקציות מקוונות כלליות או מקומיות.

בנוסף, פגיעה בפרטיות נובעת גם משימוש במגוון רחב של טכנולוגיות חדשות, במיוחד אלו המשלבות בין העולמות הפיזיים והדיגיטליים על מנת לשפר את חווית הנסיעה. השימוש במכשירים לבישים, חיישנים ואינטרנט של הדברים (IoT) בערים חכמות ויעדי תיירות חכמים, **ואיסוף רצף של נתונים בזמן אמת**, עלול להגביר או ליצור היבטים חדשים של פגיעה בפרטיות עבור המשתמשים

¹https://www.researchgate.net/publication/344444604_Impact_of_Artificial_Intelligence_in_Travel_Tourism_and_Hospitality

² <https://www.statista.com/topics/2704/online-travel-market/>

³ [https://www.techtarget.com/searchnetworking/definition/location-based-service-LBS#:~:text=A%20location%2Dbased%20service%20\(LBS\)%20is%20a%20software%20service,or%20more%20location%20tracking%20technologies.](https://www.techtarget.com/searchnetworking/definition/location-based-service-LBS#:~:text=A%20location%2Dbased%20service%20(LBS)%20is%20a%20software%20service,or%20more%20location%20tracking%20technologies.)

⁴ לדוגמה, אפליקציות תיירות מקומיות שפותחה לצרכי תיירות בעיר מילאנו:

<https://play.google.com/store/apps/details?id=guide.italy.milan.prod&hl=en>



(הנוסעים), מכיוון שהם עשויים להיות לא מוכרים או לא מודעים לצורך בהסכמתם לאיסוף ושימוש בנתונים אישיים.

האיסוף, האחסון והשימוש בנתוני מיקום, כמו גם הסיכוי לניצול לרעה של המידע הנמסר באפליקציות התיירות השונות מהווה איום מרכזי על פרטיות המידע של המשתמשים ובמיוחד לאור השימוש בשירותים מבוססי מיקום (LBS).⁵ מתוך מטרה לספק חוויות נסיעות ייחודיות, יותר ויותר ספקי נסיעות מציעים שירותים מותאמים אישית, כגון חבילות נסיעות (למשל, חבילות טיסה ומלון) המותאמות להעדפות הגלישה והרכישה של הנוסעים. כלומר, שימוש בנתוני התנהגות⁶ ונתוני התנהגות צרכנית,⁷ היכול ליצור ערך נוסף ולשפר את חווית הנסיעה הכוללת באמצעות מידע תיירותי רלוונטי, אך יכול גם לייצר סוגים חדשים של פגיעה בפרטיות עבור המשתמשים.⁸

הרשות להגנת הפרטיות ניתחה את מסמכי מדינות הפרטיות של אפליקציות מובילות בתחום התיירות ואת הצהרות אבטחת המידע והפרטיות בחנויות האפליקציות, השוותה ובחנה את דרישות ההרשאות בפועל כאשר האפליקציות מותקנות, וגיבשה סדרה של המלצות לשימוש בטוח ומאוזן תוך שמירת על פרטיות המשתמשים. יובהר כי המסמך אינו מבקש למנוע את השימוש באפליקציות אלה, אלא לתת כלים להתנהלות נכונה של המשתמשים בהיבטי פרטיות.

איסוף נתונים אישיים

אחת הסיכונים המרכזיים לפרטיות בשימוש באפליקציות תיירות טמון בעצם האיסוף והאחסון של מידע אישי רב ורגיש. כאשר משתמשים יוצרים חשבון או מבצעים הזמנה, הם לרוב מספקים מידע אישי כגון שמם המלא, תאריך לידה, מיקום נוכחי, פרטי התקשרות, ופרטי אמצעי תשלום. במהלך ההזמנה המשתמשים מספקים מידע גם על זמן הגעה ליעד, שמות הנוסעים, העדפות תזונה או רגישויות, פרטי דרכון או רישיון נהיגה. במהלך השימוש באפליקציה מתבצע איסוף מידע אוטומטי, הכולל מידע טכני על המכשיר ממנו מבוצעת האינטראקציה (כגון cookies), וכן מידע על אינטראקציה עם שירות לקוחות, שהיא לעתים קרובות אינטראקציה עם מערכת בינה מלאכותית ("בוטי"). חלק מהאפליקציות אוספות מידע גם אם לא בוצעה הזמנה, והמידע נשמר על מנת להציע

⁶ <https://journals.sagepub.com/doi/full/10.1177/0047287520951642#bibr29-0047287520951642>

⁷ Li J, Cao B. Study on Tourism Consumer Behavior and Countermeasures Based on Big Data. Comput Intell Neurosci. 2022 Jul 19; 2022: 6120511. doi: 10.1155/2022/6120511.

Altınay Özdemir, Meltem & Güçer, Evren & Bağ, Cennet. (2017). Consumer Behavior In The Process Of Purchasing Tourism Product In Social Media. İşletme Araştırmaları Dergisi. 9. 381-402. 10.20491/isarder.2017.250.

⁸ <https://journals.sagepub.com/doi/full/10.1177/0047287520951642#bibr4-0047287520951642>



למשתמש שירות בזמן מאוחר יותר. כמו כן נאספים נתוני מיקום ולעיתים מידע על מערכת תיוק הקבצים⁹ של המכשיר.

בעוד שמידע זה הכרחי למטרות ההזמנה ומתן השירות, על המשתמשים להיות זהירים ומודעים לאופן שבו נתונים אלה נאספים, מאוחסנים ומשותפים.

הסיכונים לפרטיות

נתונים רגישים רבים מועברים לספקי שירותי הנסיעה. לעתים ספקים אלו מתעלמים משיקולי אבטחת המידע האישי ובכך מגבירים את הסיכון לפרטיות המשתמשים ואת הסבירות לדלף המידע בעת התרחשות תקיפות סייבר. במחקר שנערך על ידי Security Affairs¹⁰ אשר בו נערכה ביקורת אבטחה יזומה באפליקציות המובילות להזמנת נסיעות, החוקרים מצאו מגוון רחב של ליקויי אבטחת מידע: חשיפת נתונים רגישים ומידע אישי מזהה (PII), כולל כתובות מגורים, מספרי כרטיסי אשראי וחשבונות בנק, מספרי טלפון, שמות משתמש וסיסמאות, אשר עלולים להוות סיכון פיננסי ופיזי למשתמשים כאחד.

במחקר¹¹ נוסף מצאו¹² החוקרים כי בכל הנוגע לסיכוני פרטיות, 100% מהאפליקציות שנבדקו במערכת ההפעלה של אפל לא קיבלו ציון עובר, בעוד שרק 45% מהאפליקציות שנבדקו במערכת ההפעלה של אנדרואיד עברו. ב-97% (29 אפליקציות) מאפליקציות שנבדקו במערכת ההפעלה של אפל, נמצא כי הן מסוגלות לצלם צילומי מסך של ממשק המשתמש המלא, 73% (22 אפליקציות) עשו שימוש בנתוני מיקום מדויק, בדומה לאלו המשמשים לרוב ליישומי ניווט, ו-17% (חמש אפליקציות) ניסו לקבל גישה לאנשי קשר מפנקס הכתובות. בכל הנוגע לאפליקציות הנסיעות שנבדקו במערכת ההפעלה אנדרואיד, 10% (שלוש אפליקציות) ניגשו להיסטוריית שיחות הטלפון ללא סיבה לגיטימית נראית לעין, ועוד 7% (שתי אפליקציות) השתמשו בספק תוכן לא מאובטח.

⁹ מבנה מערכת קבצים היררכית המנהלת את הנתונים והקבצים במכשיר.

¹⁰ <https://privacysavvy.com/news/research/popular-travel-apps-exposing-sensitive-data-of-millions-users/>

¹¹ <https://get.zimperium.com/security-and-privacy-issues-found-in-popular-travel-apps/>

¹² החוקרים בדקו 30 יישומי תיירות הכוללים טיסות, מלונות, השכרת רכב וכדומה, כדי להבין טוב יותר כיצד הם מנהלים את פרטיות המשתמשים ואת סיכוני האבטחה. האפליקציות נבחרו על פי כמות ההורדות מחנות Google Play וביקורות חיוביות במערכת ההפעלה של אפל. האפליקציות זכו לציונים שחושבו באמצעות מנוע ניתוח יישומים מתקדם (z3A) בשלוש קטגוריות ניתוח עיקריות: אבטחת יישומי אינטרנט (OWASP 10), שיטות עבודה מומלצות לפיתוח יישומים לנייד, ונתוני פרטיות וסיכוני אבטחת מידע. בתחום הפרטיות, הניתוח כלל את הגישה של האפליקציה לנתונים האישיים של המשתמש, מזהי מכשירים ייחודיים, SMS, תקשורת ואחסון נתונים. ניתוח סיכוני האבטחה כלל פונקציונליות ושימוש בקוד, יכולות יישומים וחולשות קריטיות. כל אפליקציה דורגה בסולם של 0 עד 100 (מהסיכון הנמוך אל הגבוה).



בכל הנוגע לאבטחת המידע ציינו החוקרים כי 100% מהאפליקציות של מערכת ההפעלה iOS נכשלו גם כאן, ואלו של אנדרואיד עם שיעור כשל של 97%. כל 30 אפליקציות הנסיעות של מערכת ההפעלה iOS השתמשו בשיטת אימות שיכולה לאפשר לתוקפים ליירט תקשורת של נתונים רגישים בין האפליקציה לאינטרנט. 7% נוספים (שתי אפליקציות) הטמיעו שיטת התקנה שעוקפת את תהליך הסקירה של אפל בחנות ההורדות וכך אפשרו פוטנציאל התקנה של תוכנות זדוניות.

מחקר¹³ עיתונאי של Cybernews מצא¹⁴ כי יש גם פערים בין ההצהרות של המפתחים בחנות האפליקציות לבין ההרשאות הנדרשות בפועל. הדבר מעלה את הסיכון לפרטיות מכיוון שהמשתמש אינו מודע לכך שישנן הרשאות שהאפליקציה מבקשת לעיתים באופן אוטומטי.

ניתוח של דלפי מידע¹⁵ והתקפות סייבר המופיעות בעיתונות מראה שמגזר זה פגיע מאוד לתקיפות סייבר, בעיקר בשל הפיצול ומורכבות רשתות הזמנת הנסיעות והתשלומים, המערבות שחקנים רבים ונותני שירותים של צד שלישי, כמו גם הגנות לקויות. מניתוח מערכות ה-IT, ונקודות המכירה

¹³ <https://cybernews.com/privacy/top-travel-apps-privacy/>

¹⁴ במחקר נבדקו 22 אפליקציות תיירות הנמצאות בשימוש נרחב, שהורדו על ידי מיליוני משתמשים בחנות Google Play, כדי לקבוע לאילו נתונים הם ניגשים ועשויים לאסוף.

¹⁵ <https://www.cyberdaily.au/security/9998-australian-travel-agency-exposes-customer-data-after-leaving-database-publicly-accessible>

<https://iapp.org/news/b/new-zealand-travel-company-announces-data-breach-of-its-old-website>

<https://www.jdsupra.com/legalnews/brownell-travel-confirms-november-2023-4500623/>

<https://www.bitdefender.com/blog/hotforsecurity/travel-industry-giants-failed-to-secure-their-websites-despite-high-profile-data-breaches-new-research-shows/>

<https://www.cyberneticgi.com/2024/02/03/how-inspiring-vacations-data-breach-affected-112000-travellers/>

<https://www.twingate.com/blog/tips/easyjet-data-breach>

<https://www.travelweekly-asia.com/Travel-News/Travel-Technology/560-million-customer-data-breach-tied-to-Taylor-Swift-tour-sales>

https://techcrunch.com/2023/09/06/ransomware-gang-claims-credit-for-sabre-data-breach/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xILmNvbS8&guce_referrer_sig=AQAAAaphnjaR_ENaIU-aGa1pQFSheoh_WbXQaYFh-L9aTm1NVezLca9eI3u8IAI5S-Pgd9XVqU6gKSIyPpDXp5-xlbKmqJ_EnZWTOKXjoFKTmnlo-pLy1q4qNVbEsiXhW785TR6ZvwYVPgjOqKIALc1APjgHf2QPWG5-b9vFVfYmKXOr

<https://www.bleepingcomputer.com/news/security/hotel-hackers-redirect-guests-to-fake-bookingcom-to-steal-cards/>

<https://www.forbes.com/sites/suzannerowankelleher/2023/09/13/ransomware-attack-mgm-resorts/>



הוותיקות (POS), נראה כי מיליוני המשתמשים מקיימים אינטראקציה עם חברות התיירות במרחב הווירטואלי ומבצעים טעויות אנוש רבות.

המלצות להתנהלות הציבור בעת שימוש באפליקציות תיירות

סקירה והתאמת ההרשאות של האפליקציה

בדקו והתאימו באופן קבוע את ההרשאות של האפליקציות שלכם. נמצא כי לעיתים ישנו הבדל בין הצהרות המפתחים בחנויות הורדת האפליקציה לבין ההרשאות אשר האפליקציה מבקשת בפועל. מומלץ לבצע בדיקה עיתית אילו הרשאות נדרשות לאפליקציה ולהתאים אותן לרמת הצורך שלכם מהאפליקציה.

הגבלת איסוף מידע על נתוני מיקום

כנסו להגדרות האפליקציה ושנו את ההרשאות כך שהגישה למיקום תוגדר ל"תוך שימוש" או "רק תוך כדי שימוש באפליקציה", במקום "תמיד".

קישוריות לרשתות חברתיות

הימנעו ככל האפשר מקישור בין האפליקציה לבין חשבונותיכם ברשתות החברתיות.

אבטחת מידע

הקפידו על כך שגרסאות התוכנה והאפליקציה שלכם יתעדכנו באופן אוטומטי, בכדי להבטיח את הגדרות הפרטיות והאבטחה העדכניות ביותר.

השלכות טכנולוגיית בינה מלאכותית

אפליקציות תיירות רבות משלבות כיום טכנולוגיות בינה מלאכותית, בין היתר כדי לשפר את חווית המשתמש. תוכנות בינה מלאכותית דורשות לעתים קרובות גישה למגוון רחב יותר של מידע אישי, כולל העדפות ונתוני התנהגות. שימו לב להרשאות אלה והתאימו אותן בהתאם לרמת הצורך שלכם מהאפליקציה.

סיום שימוש באפליקציה ומחיקת מידע

אם נראה כי לא תדרשו יותר לשירות, או שהחלטתם להפסיק להשתמש באפליקציה, מחקו את החשבון וגם את האפליקציה ובקשו מספק השירות למחוק את הנתונים שלכם. כך תבטיחו כי האפליקציה אינה ממשיכה לאסוף מידע מהמכשיר.