

צמצום הסיכונים העסקיים הנובעים משימוש בכלי AI דוגמת ChatGPT

AI | ChatGPT | Risk Management | Security

מוטי קריספיל | Storytelling, Growth & AI Strategies for Leaders



מ12 גרסה 110523

חשיפות וסיכונים פוטנציאליים (המחשות חלקיות)

- ◀ פגיעה במוניטין שלכם או של המותג עקב שילוב עובדות / נתונים מופרכים, או לא מדויקים שייצרו הכלים הללו, בתכנים שיווקיים ומסחריים שלכם דוגמת ברשור, אתר, פרסום. כן, נכון להיום כלי AI לעתים (לא נדירות) "ממציאים" עובדות, נתונים, סימוכין או מחקרים/ציטוטים
- ◀ **גניבת מידע** פרטי/מסחרי, כולל גניבת זהויות ותוכן צ'אט עקב **פריצה לשרתים** של השירות בו אתם משתמשים
- ◀ **חשיפה משפטית** ורגולטורית עקב שימוש במידע לא נכון
- ◀ **זליגה של מידע קנייני/סודי-מסחרי** של לקוח שלכם, אותו שילבתם במהלך ההתכתבות, עקב פריצה
- ◀ זליגה של מידע קנייני/סודי-מסחרי שלכם או של לקוח שלכם, כחלק מובנה ממנגנון "האימון" והלמידה של הכלי

הצורך

- ◀ אתם והעובדים שלכם משתמשים בכלי AI דוגמת ChatGPT למטרות שיווקיות, ניהוליות, מסחריות ואחרות, כמו כולם...
- ◀ **"הצד האפל" של השימוש בכלים אלו עלול לחשוף את העסק שלכם לסוגיות פוטנציאליות של פרטיות, זליגת מידע קנייני, גניבת מידע עסקי, ועוד.**
- ◀ אתם מעוניינים להמשיך ליהנות מהיתרונות בשימוש בכלים אלו אך לצמצם עד כמה שאפשר את החשיפות והסיכונים הללו

מדוע אנו חשופים כל כך? דברים שחיוני לכל מנהל לדעת!



- ◀ אנו עדים לצונאמי של עשרות ומאות השקות מוצרים ושירותים בני שבוע, בשבוע! שמציעים שירותים מבוססי AI
- ◀ במקרים רבים אין למפתחים הללו (לעתים מפתח יחיד או סטארטאפ קטן) מושג **איך להגן על היישום נגד אינטימיות, Privacy, Security**, ופריצות אליהם. הם פשוט נחפזים לשחרר כלים חדשים במרוץ החימוש הזה. פורצים (כולל אלו שמועסקים על ידי מתחרים פוטנציאליים) יכולים לגשת למידע רגיש שלכם, כולל מסמכים ששיתפתם, הסטוריית שיחות, ומה לא
- ◀ המשתמשים בכלים הללו, לרוב אינם בעלי רקע טכנולוגי (שיווק, תפעול, מכירות, מרקום, כספים, הנהלה וכו'), אינם מומחי אבטחה או AI. הם פשוט משתמשים בכלי **באמונה (לא מבוססת)** שהכל יהיה בסדר ושהמידע האישי שלהם, כמו גם התכנים שהם משתפים, נשמר פרטי, מוגן ובטוח
- ◀ **גרוע מכך:** חלק מהכלים **משתמש באופן מוצהר** כחלק מהפונקציונליות שלו במידע הרגיש ששיתפתם כדי לאמן ולשפר את דיוק התשובות, בכדי לתת בהמשך תשובות טובות **לאחרים!**
- ◀ האופן בו אתם "משוחחים" עם ChatAI (בשונה מחיפוש ב-Google) **מסגיר הרבה יותר מידע רגיש שלכם** על כוונות, אסטרטגיה, יכולות מוצר, תוכניות פעולה, יתרונות תחרותיים של דברים שאתם עובדים עליהם. כל זה, פוטנציאלית, חשוף לגניבה/פריצה, או ישמש את הכלי לאימון לטובת אחרים...
- ◀ ועוד ועוד... אבל אני חושב שהבנתם את עומק החשיפה...

בעמוד הבא אשתף בטיפים מעשיים לצמצום הסיכונים והחשיפות





הנוסחה

הדריכו את העובדים שלכם (ואתכם, כעובד מס' 1) לאמץ את כללי הברזל ל "סקס בטוח" עם כלי AI

- ◀ **העדיפו באופן ברור שימוש בכלים של חברות גדולות ומוכרות**, על פני אימוץ כלים חדשים של מפתחים לא מוכרים, גם אם אלו האחרונים מציעים יתרונות יחסיים. הסיכון שיפרצו אליהם קטן משמעותית, ורשיונות השימוש שלהם כמו גם הגנת הפרטיות, מתועדים, ומידתיים
- ◀ לדוגמא: ב ChatGPT ניתן לבחור בהגדרות שלא לאפשר שימוש בשיחות שלכם לאימון הכלי
- ◀ **אסור לשתף מידע קנייני / רגיש של החברה / המוצר / הלקוח בכלי Chat AI**
- ◀ **זייפו עובדות:** החליפו את שם המוצר או החברה שלכם בשמות פיקטיביים במהלך השיחות
- ◀ אם אתם נעזרים בכלי לטובת מוצר/שרות חדש, נסחו את **השאלות באופן כוללני יותר**
- ◀ **לדוגמה:** במקום לשתף שאתם רוצים ליצור תוכן על רובוט סודי שמזהה **מצבי מצוקה בקרב קשישים**, חפשו מידע / ייצרו תכנים על רובוטים **שמזהים רגשות** באופן כללי, ובצעו התאמות מאוחר יותר בקבצים הפרטיים שלכם
- ◀ **בדקו היטב את התשובות:** אם אתם נעזרים בכלי למחקר, תקפו כמה פעמים את התשובות. הצליבו מול Google וחפשו את המחקרים, את העובדות, את המקורות.
- ◀ הדבר האחרון שאתם רוצים לגלות הוא שהדוח האחרון שהפצתם למאות לקוחותיכם מכיל עובדות לא מדויקות
- ◀ דרשו מעובדיכם **לקבל אישור מוקדם** על שימוש בכלים חדשים וצעירים שלא ברור מי המפתח, מה רמת ההגנה ושמירת הפרטיות שלכם, ומהן האותיות הקטנות...
- ◀ **פצלו את השיחות** למספר לשוניות נפרדות, ומזגו את התשובות לתוך המסמך שלכם, בפרטיות שלכם
- ◀ **מנו איש טכני / איש IT להיות מעין "מבוגר אחראי"** לשימוש בכלים, להדרכה בשימוש נכון, ולבדיקה של כל כלי: מי המפתח, מה החשיפות שנתגלו על ידי אחרים, וכדומה. בקשו ממנו להתעדכן תדירות בכתבות על פריצות, איומים, וכדומה.
- ◀ **הדריכו כל עובד חדש**, או ספק / **Freelancer** בנוגע לכללים שאתם מצפים ממנו שיישם עם המידע שאתם מספקים לו
- ◀ בדקו והעדיפו לאמץ כלים שיאפשרו לכם **להריץ מקומית Chat AI**. כלים כאלו מתחילים להופיע בשוק, ויש להתעדכן מעת לעת.
- ◀ **רגישות יתר בסוגיות של פטנטים:** אל תשתפו תכנים שקשורים בפטנטים בתהליך. אתם עלולים לסכן בעתיד את תקפות ראשוניות הקניין