Google

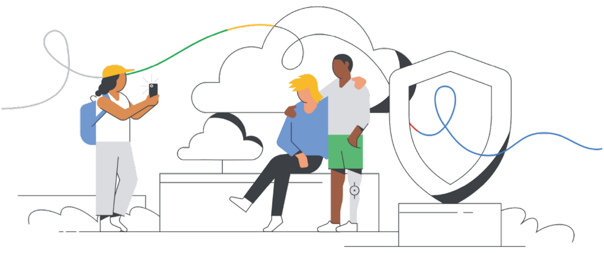
המסע שלנו באבטחת סייבר לאורך השנים

Safer with Google

אנחנו שומרים על אנשים בטוחים יותר באינטרנט

לנוכח העלייה הדרמטית בגורמים זדוניים באינטרנט ובמתקפות סייבר במימון מדינות, אנחנו מאמינים שאבטחת המוצרים והשירותים שלנו חשובה לא פחות מיעילותם.

אנחנו ב-Google ממוקדים כיום יותר מאי פעם בהגנה על אנשים, ארגונים וממשלות – אנחנו שואפים לשתף מהידע שלנו, להעצים את החברה לטיפול בסכנות הסייבר המתפתחות מהר מתמיד ולקדם פיתוח שוטף של אבטחת סייבר ברמה הגבוהה ביותר, במטרה ליצור עולם בטוח יותר לכולם.



לא מפסיקים לחדש ולהתחדש

מאז השקת Gmail ב-2004 ועד המחשוב המוגן ב-2022, Google תמיד הייתה חלוצה בפיתוח טכנולוגיות של אבטחת סייבר וכל הזמן חידשה עם מוצרים, פלטפורמות ושותפויות, במטרה לסכל קטגוריות שלמות של איומים וליצור עתיד בטוח יותר לחברות, לארגונים ולאנשים על ידי:

- ✓ פיתוח פלטפורמות ומוצרים מאובטחים
- ✓ הקמת צוותי אבטחה גמישים
- ✓ טיפוח תוכניות ושותפויות
- ✓ מימון קריט של חידושים והדרכות לעובדים

ככל שצורכי האנשים והאינטרנט מתפתחים, כך גם אנחנו ממשיכים להיות בחזית הטכנולוגית כדי לסכל את איומי הסייבר המשתנים ולוודא שכל יום בטוח יותר בעזרת Google.

2004
– הגנה על ספאם ב-Gmail

היינו אחת מהחברות הראשונות לפתח הגנות באימייל שמבוססות על בינה מלאכותית.

99.9% מהאימיילים החשודים והמסוכנים נחסמים על ידי Gmail

2007
– גלישה בטוחה

אנחנו עוזרים באופן יזום להגן על מכשירים בכל העולם באמצעות התראות למשתמשים כשהם נכנסים לאתרים מסוכנים, וב-2020 פיתחנו את ההגנות האלה באינטרנט ויצרנו גרסה משופרת של גלישה בטוחה.

5 מיליארד מכשירים בעולם מוגנים על ידי גלישה בטוחה

2008
– מנהל הסיסמאות של Google

בזכות השקת מנהל הסיסמאות, קל ובטוח יותר להיכנס לחשבון, כי לא צריך לזכור או להקליד את הסיסמה. משתמשים בו כיום ב-50% מהכניסות לחשבונות בפלטפורמות השונות של Chrome.

מיליארד סיסמאות נבדקות
מדי יום כדי לזהות אם הן דלפו

2009
– reCAPTCHA

רכשנו את הפתרון לניהול הונאות ובוטים כדי לסכל דחיפת סיסמאות (credential stuffing) והשתלטויות על חשבונות, וכדי למנוע פעילות עוינת מצד תוכנות זדוניות/משתמשים מזויפים.

5 מיליון אתרים מוגנים

2010
– אפס אמון

אחרי שסיכלנו את מבצע אורורה, סדרה של מתקפות סייבר מתואמות, עשינו מהפך בגישה ויצרנו ארכיטקטורה של אבטחה כברירת מחדל בשם 'אפס אמון'. בזכותה יש פחות וקטורים של תקיפה, פחות הזדמנויות לאבד מידע ויותר שליטה על המערכות שמשתמשים תלויים בהן. אנחנו תומכים במאמצי הבית הלבן לפרוס את מודל האבטחה 'אפס אמון' במשרדי הממשל הפדרלי, ושילבנו אותו גם בפתרון האבטחה שלנו BeyondCorp Enterprise כדי שכל ארגון יוכל להיעזר בו.

2010
– צוות לניתוח איומים (TAG)

אחרי מבצע אורורה, הקמנו צוות מיוחד של מומחים שאחראים על זיהוי, ניתוח ושיבוש איומי סייבר חמורים במימון ממשלות. הצוות הצליח להתחקות אחרי WannaCry, המתקפה הגדולה בהיסטוריה של תוכנת כופר, עד לקוריאה הצפונית, ולאחרונה שיתף דוגמאות למערכות של השכרת האקרים מהודו, מרוסיה ומאיחוד האמירויות.

2010
– ציידי הבאגים של Google

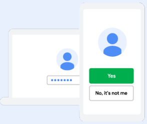
תוכנית התמריצים שלנו לזיהוי נקודות חולשה מושכת תלמידים, עורכי דין, מומחים טכנולוגיים וחובבים לצוד באגים במוצרי Google ולקבל כסף בתמורה. המוטיבציות שלהם רבות ומגוונות, אבל המטרה זהה: לאתר נקודות חולשה שלא זיהינו כדי לשמור על אבטחת השירותים באינטרנט.

מיליוני דולרים שולמו כתמריצים מאז 2010

2010
– הצוות האדום

הצוות הושק בשביל לפרוץ ל-Google, כדי להבין איך עובדות המתקפות, ולעזור לנו לחזק את חומות ההגנה ולאתר פרצות. חבריו פועלים בכל העולם כדי להיות עם יד על הדופק בקשר לאיומים הקיימים, לשפר את מנגנוני האבטחה, לזהות ולמנוע מתקפות ולסכל קטגוריות שלמות של נקודות חולשה על ידי קידום מסגרות עבודה חדשות ומשופרות.

2011
– אימות דו-שלבי



היינו בין הראשונים להציע אימות דו-שלבי (2SV) כברירת מחדל, והראשונים להפעיל אותו אוטומטית עבור יותר מ-150 מיליון אנשים ב-2021, כדי לאפשר כניסה קלה ובטוחה לחשבון. בזכות זה, גם אם הסיסמה נגנבת, החשבון מוגן.

50% ירידה בחשבונות שנפרצו מאז
הוספת האימות הדו-שלבי

2013
– Project Shield

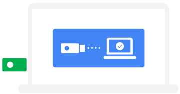
בעזרת Project Shield, גופי חדשות, ארגוני זכויות אדם, אתרי בחירות, ארגונים פוליטיים וקמפיינים היו מוגנים מפני מתקפות סייבר של מניעת שירות מבוזרת (DDoS) ביותר מ-100 מדינות – והכול בזכות זיהוי איומים והפעלת מענה מצד קהילת האבטחה ורשויות אכיפת החוק.

יותר מ-150 אתרים מוגנים
כיום באוקראינה

2014
– Project Zero

הקמנו כוח משימה מיוחד שמטרתו לצוד נקודות חולשה שמאפשרות מתקפות אפס ימים באינטרנט – בתוכנה, בחומרה, במוצרי Google ובמקומות נוספים – כדי לשמור על האינטרנט בטוח ופתוח. חבריו היו הראשונים לדווח על נקודות החולשה Meltdown ו-Specter במעבדים, ואפשרו למפתחים לטפל בהן ולהטמיע תיקונים בשרשרת אספקת התוכנה.

2017
– תוכנית ההגנה המתקדמת (APP)



הוספנו מנגנוני אבטחה, כולל מפתח אבטחה, לאישים בולטים ומשתמשים שנמצאים בסיכון גבוה, כמו עיתונאים ופקידי ממשל.

יותר מ-300 קמפיינים פדרליים
מוגנים

2017
– Google Play Protect

Google Play Protect, השירות הנפוץ ביותר בעולם להגנה על איומים בנייד, שכל הזמן מותאם ומשתפר בעזרת יכולות למידת המכונה של Google, סורק אוטומטית אפליקציות בחיפוש אחר תוכנות זדוניות ומצפין את תשלומי המשתמשים בטלפונים עם Android.

יותר מ-100 מיליארד אפליקציות
נסרקות מדי יום בחיפוש אחר תוכנות זדוניות

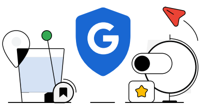
150 מיליון תשלומי
משתמשים מוצפנים מדי יום

2018
– מפתח האבטחה Titan

יצרנו את מפתח האבטחה Titan למשתמשים שרוצים פתרון של Google מקצה לקצה. המפתחות תואמים ל-FIDO ואפשר להשתמש בהם לא רק ב-Google, אלא גם במקומות נוספים.

2019
– אימות מחדש ללא סיסמה

הרחבנו את התמיכה שלנו ב-FIDO למשתמשי Android, כך שהם יוכלו להיכנס לחשבון באתרי אינטרנט בצורה חלקה רק עם קוד סודי או כניסה ביומטרית, בלי סיסמה.



2019

– Chronicle

Chronicle, הבנוי כשכבה מיוחדת מעל תשתית הליבה שלנו, הושק כדי לספק אבטחה בענן לארגונים שרוצים לשמור, לנתח ולחפש בצורה פרטית כמויות ענק של נתוני אבטחה ורשת.

2021

– השקעה באבטחת סייבר מתקדמת

חרטנו על דגלנו לחזק את אבטחת הסייבר, להרחיב את התוכניות של אפס אמון, לעזור באבטחה של שרשרת אספקת התוכנה ולשפר את האבטחה בקוד פתוח. התחייבנו להכשיר 100,000 אמריקאים בתחומים כמו תמיכה טכנית וניתוח נתונים, באמצעות תוכנית ההסמכות המקצועיות של Google.

מחויבות להשקעת **10 מיליארד דולר** ביוזמות של אבטחת סייבר

2021

– Confidential Computing

השקנו את Google Cloud Confidential Computing, טכנולוגיה מהפכנית לאבטחה, בטיחות ופרטיות ברמות קריטיות, ששומרת על הצפנת הנתונים בזמן שהם מעובדים, ועל אבטחתם לאורך כל מחזור החיים, כולל כשהם באחסון או במעבר. כיום גם את הנתונים הרגישים ביותר אפשר להעביר בבטחה לענן.

2021

– הצוות של Google לאבטחת קוד פתוח (GOSST)

הקמנו את GOSST כדי לשפר את האבטחה של תוכנות בקוד פתוח שנעזרים בהן בכל רחבי העולם. חברנו לקרן לאבטחת קוד פתוח (OpenSSF) כדי לפתח ולהפיץ רמות של שרשרת אספקה לארטיפקטים של תוכנה (SLSA), מסגרת לאבטחה של שרשרת אספקת התוכנה ולשמירה על אבטחת כלל מערך התוכנה בטווח הארוך.

מחויבות להשקעת **100 מיליון דולר** בפעולות אבטחה של צד שלישי בקוד פתוח, כדי לעזור בתיקון נקודות חולשה

2022

– תקן להצפנה פוסט-קוונטית

במבט לעתיד, אנחנו ממשיכים לפתח את הדור הבא של מערכות ההצפנה, כדי להגן מפני פריצה למערכות הצפנה של מפתחות ציבוריים ולמנוע סכנות בתקשורת דיגיטלית. מכון התקנים והטכנולוגיה האמריקאי בחר, במעורבות של Google, באחת מההצעות לתקן (SPHINCS+).

2022

– Protected Computing

בישרנו על Protected Computing – ערכת כלים טכנולוגיים שכל הזמן מתרחבת ומשנה את הדרך, התזמון והמיקום שבו המידע מעובד כדי שהוא יישמר פרטי ומאובטח. הכלים מבוססים על עקרונות של מזעור טביעת הרגל במידע, אנונימיות המידע והגבלת הגישה למידע רגיש. כך, למשל, אנחנו יכולים להציע במכשירי Android רעיונות לכתיבת והשלמת הודעות, תוך שמירה על פרטיות מלאה בשיחה.

2023

– מפתחות גישה: הדרך לעתיד ללא סיסמאות

במשך עשור הכנו את הקרקע לעתיד ללא סיסמאות: https://safety.google/cybersecurity-advancements/. הצטרפנו לברית FIDO ב-2013 כדי לקדם תקנים פתוחים לעולם ללא סיסמאות, וכיום, בזכות הרחבת התמיכה בתקני כניסה לחשבון של FIDO ב-Android וב-Chrome באמצעות הטכנולוגיה של מפתחות גישה ב-2023, סוף כל סוף יש לנו את הפלטפורמה שתאפשר עתיד ללא סיסמאות.

2022

– Madiant ו-Google Cloud

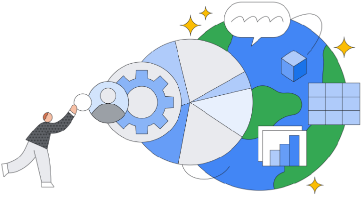
Mandiant הוא גוף לאיסוף מודיעין עומק בזמן אמת על איומים מחזית אבטחת הסייבר בעזרת הארגונים הגדולים ביותר בעולם. בשילוב עם פתרונות האבטחה המובנים של Google Cloud, אנחנו עוזרים לארגונים ולגופים מהמגזר הציבורי להיות מוגנים לאורך כל מחזורי חיי האבטחה.

בעידן שבו הטכנולוגיה מגיעה כמעט לכל מקום, האמון בטכנולוגיה קריטי למימוש הפוטנציאל האמיתי של החברה האנושית.

כשאנחנו מיישמים את הידע שלנו באבטחה, אנחנו כל הזמן חוברים לאנשים, לעסקים ולממשלות כדי להגן על אבטחתם ולהוביל לעידן חדש באבטחת סייבר.

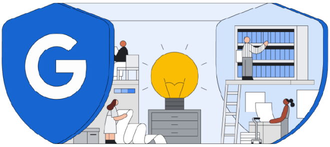
הגנה על אנשים, עסקים וממשלות

אבטחה היא אחד מעקרונות היסוד באסטרטגיית פיתוח המוצרים שלנו. לכן כל המוצרים שלנו מכילים מנגנוני הגנה מובנים, שהופכים אותם למאובטחים כברירת מחדל.



העצמת החברה האנושית כולה לטיפול בסכנות המתפתחות של אבטחת סייבר

אנחנו מעודדים ומעצימים קהילות לממש את הפוטנציאל שטמון בקוד פתוח, ומשתפים את הידע והמומחיות שלנו בצורה שקופה עם כלל הגורמים בתחום, כדי שכולם יהיו בטוחים יותר.



קידום העתיד הטכנולוגי

אנחנו רוצים להגן על בני האדם מהדור הבא של איומי סייבר. אנחנו נשענים על המומחיות שלנו בבינה מלאכותית ומפתחים את הגל הבא של ארכיטקטורות כדי לפרוץ את גבולות החדשנות באבטחה.

מדי יום ביומו, אתם בטוחים יותר עם Google

היכנסו לאתר g.co/safety/cyber

Google