

Social Engineering

And Information gathering

By Roy Saar

הגדרה

- פעולת המניפולציה על אדם על-מנת לגרום לו לממש את מטרותינו. פעולה זו כוללת איסוף מידע, מתן אישור כניסה או לגרום לאדם לבצע פעולה מסוימת עבורנו.
- הנדסה-חברתית היא "People Hacking" אשר כוללת ניצול האמון אשר נותנים בני האדם אחד בשני.
- בכל פעם שאתה גורם לאדם לעשות משהו עבורך אתה מפעיל הנדסה-חברתית. החל מילד שמקבל פיצה בחינם או משכנע את הוריו לקנות לו צעצוע עד ללגרום לאדם לתת לך את סיסמת האדמין שלו.
- הנדסה חברתית היא אמנות, והיא קשה לרכישה וללימוד. בנוסף קשה מאוד להגן ממנה, היא מסובכת להפליא, אך נותנת תוצאות מדהימות.



Social Engineering at McDonalds - Free cheeseburger &
@fries

Kevin Mitnick



A professional headshot of Frank Abagnale. He is a middle-aged man with thinning grey hair, smiling warmly at the camera. He is wearing a dark navy blue suit jacket, a white dress shirt, and a patterned tie with a grid-like design in shades of grey and white. The background is a textured, mottled teal or blue-green color.

Frank Abagnale

מה אנחנו רוצים?

- סיסמת אדמין?
- אישור כניסה \ תג עובד?
- מפתחות לבניין או לחדר מחשבים?
- דוחות כספיים?
- פרטי עובד?
- רכוש פרטי של חברה (דגמים, תוכנות, קוד, גראפים)?

שעת סיפור מאת אירה ווינקלר

צעד אחר צעד

- איסוף מידע
- בניית אמון
- ניצול האמון \ מערכות היחסים \ המידע שנאסף \ נחמדות בני האדם \ טיפשותם.

Google

חיפוש מפות

חיפוש ממשל

חיפוש אנשים

חיפוש עסקים



ישוב (למשל רמת גן)

'1=1' or -- |

שם פרטי ומשפחה (למשל אבי כהן)

'1=1' or -- |

בלחיצה על כפתור החיפוש אני מסכים לתנאי השימוש באתר

חדש ב-b144

מהיום, ממשק חיפוש חדש באתר: **חיפוש מיקוד** הממשק מאפשר לבצע חיפוש מיקוד של עסקים ואנשים על פי כתובת, בצורה הפשוטה והמהירה ביותר.

שירות לעסקים

- פרסום במדריך B144
- כניסת מנויים
- תנאי שימוש למסויים
- תנאי שימוש לבניית אתרים

מידע

- אודות השירות
- שאלות ותשובות
- תנאי שימוש באתר
- חדש באתר
- שת"פ בזק אמון הציבור
- מספרי חירום
- חיפוש מיקוד

כלים

- אינדקס תחומים
- צור קשר
- שמירה למועדפים
- מקלדת וירטואלית
- נגישות
- המלצות לצרכנות נבונה
- רשימת העסקים שלי



בוקס עסקים





CAUTION
DO NOT PLAY IN, ON
OR AROUND OR OCCUPY
THIS CONTAINER
FOR ANY PURPOSE.

WAA

2yd



איסוף מידע ב-3 דקות

משחק ילדים

חיפוש waze

חיפוש מתקדם (2,020,000 תוצאות (0.08 שניות))

Free GPS Navigation with Turn by Turn - Waze

waze is a free mobile navigation application for your iphone or android that allows drivers to build and use live maps, real-time traffic updates and ...
www.waze.co.il/ - עותק שמור - דפים דומים

מפה חיה לוח הבקרה שלי
הורדה סיוור מודרך
ישראל Waze קהילה
תמיכה אודות

עוד תוצאות מ- waze.co.il

Traffic Jam News, Updates from the Road - Waze Live Map

שרת **Waze** החזיר שגיאה לפעולה זו. לא ניתן ליצור קשר עם שרת **Waze**. התרחשה שגיאה ...
www.waze.co.il/livemap/ - עותק שמור - דפים דומים

Waze - הורדה

הורידו את **Waze** לסלולרי החכם שלכם. זה פשוט, מהיר וחינם. **Waze** הוא שרות סלולרי ...
www.waze.co.il/download/ - עותק שמור - דפים דומים

Waze ישראל

שרת **Waze** החזיר שגיאה לפעולה זו. לא ניתן ליצור קשר עם שרת **Waze**. התרחשה שגיאה ...
www.waze.co.il/wm_symbian_download/ - עותק שמור - דפים דומים

הצג תוצאות נוספות מ- waze.co.il

Waze – Social GPS navigation, traffic & road reports for iPhone ...

[תרגם דף זה] -
Waze is a free social traffic and navigation app that uses real-time road ... 23 Mar 2011
reports from drivers nearby to save commuting time and improve ...
itunes.apple.com/us/app/id323229106?mt=8 - עותק שמור - דפים דומים

ynet מחשבים - Waze - שירותי ניווט ודיווח על פקקים בחינם

5 ינואר 2009 ... תוכנת הניווט FreeMap מיתגה את עצמה מחדש בשם **Waze**. תוכנה שמציעה עדכונים



- הכל
- תמונות
- סרטונים
- חדשות
- בלוגים
- עוד

- חפש באינטרנט
- חפש דפים בעברית
- דפים זרים מתורגמים
- כל זמן
- עדכון אחרון
- ב-24 השעות האחרונות
- בשבוע האחרון
- בחודש האחרון
- בשנה האחרונה
- טווח מותאם אישית...
- עוד כלי חיפוש

אורי הוא בוגר תואר ראשון בכלכלה מאוניברסיטת תל אביב.



אהוד שבתאי | מייסד-שותף, סמנכ"ל טכנולוגיות

אהוד שבתאי הוא המייסד והיוזם של פרויקט Freemap שנהמשך לו הוקמה Waze. אהוד פעיל מאוד בקהילת הקוד הפתוח עם רקע מגוון בתשתיות, פיתוח וטכנולוגיות תוכנה רבות. לפני שהקים את Waze אהוד היה סמנכ"ל הטכנולוגיות של חברת X.L.Net Ltd. ולפני כן מילא תפקידי פיתוח בכירים בחברות Ascent PI וקומברס.



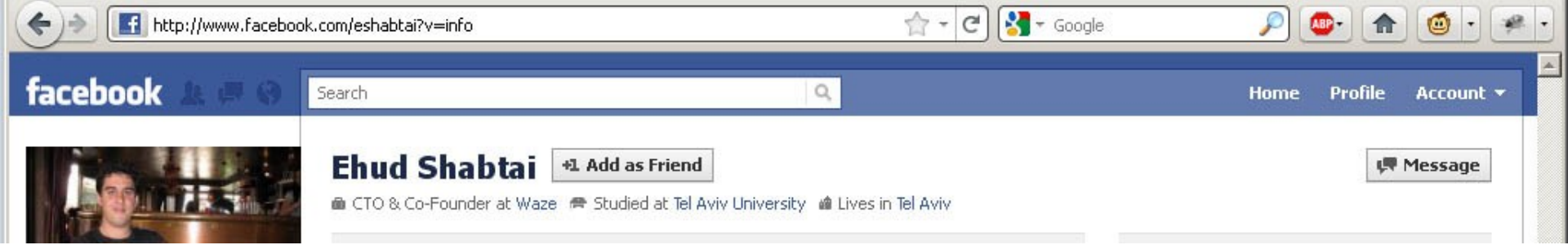
אהוד הוא בוגר תואר ראשון במדעי המחשב ותואר ראשון בהצטיינות בפילוסופיה, שניהם מאוניברסיטת תל אביב.

אמיר שנער | מייסד-שותף, סמנכ"ל מחקר ופיתוח

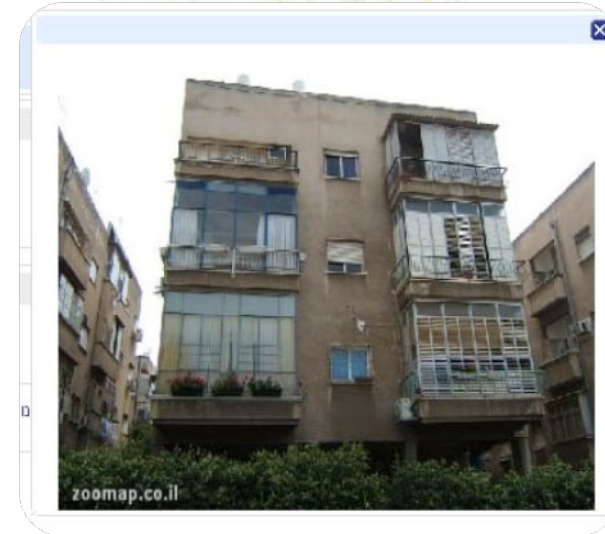
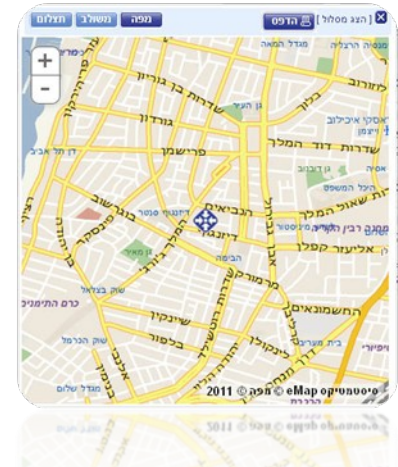
אמיר, מייסד-שותף ב-Waze, תורם לחברה מעל 15 שנות ניסיון כארכיטקט, מפתח בכיר ומנהל מחקר ופיתוח וכיום מוביל את קבוצת הפיתוח בחברה. אמיר הפך לשותף בהקמת Waze לאחר שייסד והיה המנכ"ל של חברת X.L.Net Ltd., פתרון תוכנה מותאם אישית. לפני כן שימש כמנהל מחקר ופיתוח בקומברס, עם התמחות בטכנולוגיות קוד פתוח.



לאמיר יש תואר ראשון בהצטיינות בהנדסת חשמל ומדעי המחשב ותואר שני בהנדסת חשמל, שניהם מאוניברסיטת מינסוטה.



- **תיכון:** עירוני ה', תל-אביב.
- **אוניברסיטה:** ת"א תואר ראשון במדעי המחשב ופילוסופיה.
- **עבד ב:** Freemap, X.L.Net, Ascent PI, Comverse, Waze.
- **כתובת בעבודה:** רחוב הסדנא 2, רעננה.
- **טלפון בעבודה:** 09-7486437.
- **מייל:** ehuds@waze.co.il
- **כתובת מגורים:** רחוב ספיר אליהו 6, ת"א.
- **נשוי:** לא.
- **טלפון פרטי:** 054-7245785.
- **תחביבים:** מחשבים, גאדג'טים, תיאטרון.



צעד אחר צעד

- איסוף מידע
- בניית אמון
- ניצול האמון \ מערכות היחסים \ המידע שנאסף \ נחמדות בני האדם \ טיפשותם.

בניית אמון

- אמון הוא תמצית ההנדסה-החברתית. הוא קשה ביותר להשגה, אך קל מדי לאבדו, ולכן עליך להיות זהיר מאוד.
- מרבית המהנדסים-החברתיים צוברים אמון בפרק זמן ארוך יחסית ובזהירות יתרה.
- "מרבית האנשים סומכים על האחר עד שתהיה להם סיבה טובה להפסיק" (קווין ביור)
- כמעט כולם מעוניינים לשתף פעולה בסביבת העבודה שלהם ויותר מזה: להיות אהובים. על-כן לפעמים שוכחים איזה מידע אסור לנדב לקולגה או "למקור אמין" 😊.

צבירת אמון לוקחת זמן.
מהנדסים-חברתיים מנוסים עושים זאת בדקות.

איך הם עושים את זה?

13

14

12

10

11

9

זהירות! קלישאה: חביבות ונחמדות

- אין יותר מספק מלעזור לאדם אדיב, מנומס ונעים הליכות, בין אם לפתוח עבורו את הדלת, ללחוץ בשבילו על כפתור המעלית או לנהל איתו שיחה קלילה. את עובדה זו חייבים לנצל – מפתיע כמה רחוק ניתן ללכת כך, שהרי מי לא אוהב אדם נחמד?
- היעזר במידע שאיגדת בשלב האיסוף על-מנת להעמיד פנים שאתה רוכש את אותם תחביבים כמו המטרה שלך, עובד בסביבתו, מתעסק באותם תחומים, או אפילו חולק את אותו השם.

**LOVE
MIE!**

התחזות

- העמד פנים כעובד חדש.
- התחזה לעובד שהמטרה עדיין לא פגשה.
- התנהג כעובד בחברה אחרת שהגיע לעשות עסקים.
- התנהג ושדר הרגשה של נינוחות, ביטחון וסמכות וכך יושפעו האנשים סביבך.

משחק והניסיון האישי שלי

- ההתמחות שלי היא Reverse Engineering, אבל בזמן התנסות ביכולות הפריצה שלי בסביבות התיכון (תיכון תלמה-יילין לאומנויות, מגמת תיאטרון) שמחתי לגלות שכישורי המשחק שלי תרמו בצורה אדירה והיו לא פחות חשובים מהיכולות הטכניות.
- התחלתי ללמוד להשתמש בשפת-גוף, וקריאה קרה וחמה בכדי להגדיל את הידע שלי כמהנדס-חברתי.
- אבל איך ניתן ללמוד להשתמש בשפת גוף? ויותר חשוב, איך ניתן ללמוד לקרוא אותה?

טכניקות מיוחדות (או: איך להפוך לשחקן בכמה דקות?)

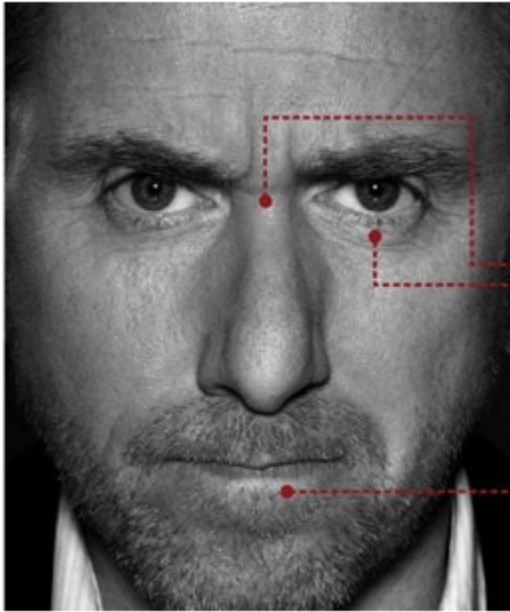
- שפת גוף: צורת תקשורת פיזית שאיננה מילולית, הכוללת: צורת עמידה, מחוות, הבעות פנים ותנועות עיניים שבני אדם מבצעים בצורה לא-מודעת.
- איך נשתמש בזה? לדוגמא, מה תוכלו לומר לי על האיש אשר:
- כוסס ציפורניים.
- עומד זקוף.
- לא מביט לאדם איתו הוא מדבר בעיניים.
- חסר-מנוחה (מקפיץ את ידיו ורגליו).
- משלב ידיים.
- עונה בהיסוס, מתעכב במתן תשובה.

טכניקות מיוחדות – פרק נוסף

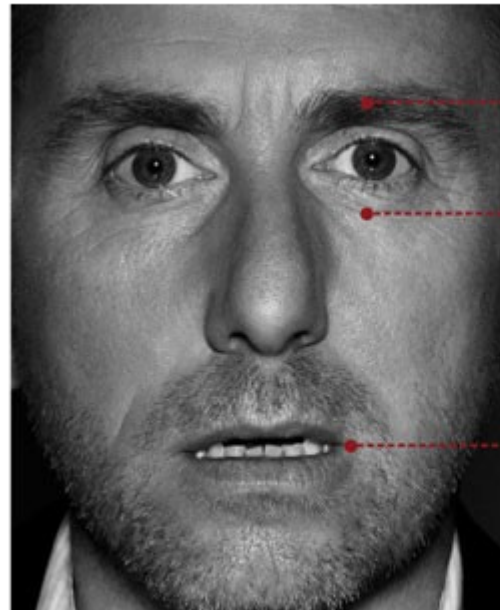
- **קריאה קרה:** שיטה אשר בה משתמשים מגלי עתידות ושאר שרלטנים. בשיטה זו אנו קוראים את האדם העומד מולנו ע"י סימנים חיצוניים הכוללים מראה והתנהגות.
- לדוגמא: על אדם שהולך עם כפכפים, תיק צד, שיער פרוע וקעקוע על הצוואר נלמד כי הוא אדם די שאנטי ונינוח, לא נדבר אליו בשפה גבוהה מדי, ונדע לתאר בקצרה מה אוהב או לא אוהב.
- דוגמא נוספת: אל אדם לבוש בחליפה, עם מזוודה שנראה מאורגן ומסודר, נדבר בנימוס ובכבוד וכך נרכש את אהבתו.
- הדברים הללו אולם נראים מובנים מאליהם, אך קריאה קרה היא טכניקה שכאשר היא מפותחת מספיק היא נראית ממש ככוח על-טבעי.
- **קריאה חמה:** טכניקה זהה לקריאה קרה, המשלבת איסוף חומר קודם על האדם אותו אנו מדובבים. האיסוף כולל קריאה ברשת, ספרים, ביוגרפיות, רשתות חברתיות וכדומה.

טכניקות מיוחדות – פרק אחרון

- הבעות פנים:
- פאול אקמן ערך מחקר וזיהה בו 7 הבעות בסיסיות המשותפות לכל בני האדם, ללא הבדל דת, גזע, מין או תרבות.
- ע"י זיהוי 7 ההבעות הנ"ל תוכל לקבל מושג אודות תחושותיו של האדם ומחשבותיו עליך.
- דוגמאות:



- ① eyebrows down and together
- ② eyes glare
- ③ narrowing of the lips

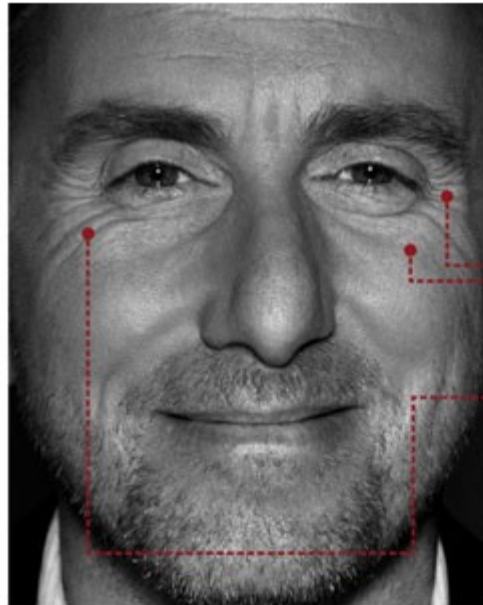


Lasts for only one second:

- ① eyebrows raised
- ② eyes widened
- ③ mouth open



- ① eyebrows raised and pulled together
- ② raised upper eyelids
- ③ tensed lower eyelids
- ④ lips slightly stretched horizontally back to ears



A real smile always includes:

- ① crow's feet wrinkles
- ② pushed up cheeks
- ③ movement from muscle that orbits the eye

טכניקות מיוחדות - פרק אחרון באמת

- **NLP**: אולי הנושא המעניין ביותר מבין כל הטכניקות שהזכרתי, אולי בגלל שאינו מוכח מדעית כטכניקה יעילה.
- הטכניקה מתארת שימוש במילים ובשפת הגוף שלנו על-מנת להחדיר לאדם איתו אנו מדברים מחשבות שלא היה חושב אילולא היינו מבצעים פעולות אלו. מחשבות אלו יכולות להפוך לפעולות.
- לדוגמא: לשאול בחורה "מתי את גומרת ללמוד?" במקום "מתי את מסיימת ללמוד?".

צעד אחר צעד

- איסוף מידע
- בניית אמון
- ניצול האמון \ מערכות היחסים \ המידע שנאסף \ נחמדות בני האדם \ טיפשותם.

Chaser's war on everything



עכשיו תורכם

תודה רבה על ההקשבה