Only amateurs attack machines; professionals target people.

Bruce Schneier

סמינר באבטחת מידע

Usability and Psychology

מרצה: פרופ' אור דונקלמן

מגיש ע"י: מוריה בן שושן

מה הקשר לפסיכולוגיה?

- האנשים הם אלו שמשתמשים במחשב
- בימינו הולכות ומתגברות התקפות המבוססות על פסיכולוגיה

Pretexting (אמתלה)

- יצירה של תרחיש מומצא על מנת לגרום לקורבן לחשוף מידע או לבצע פעולות שמשרתות את מטרת התוקף
- תקיפה של המערכת דרך המפעילים שלה (הצוות)
- בד"כ משמש לתקיפה של חברות, אך לאחרונה משמש גם לתקיפה של אנשים פרטיים

דרכי התמודדות

- אימון הצוות
- קביעת כללים ותנאים למסירת מידע חסוי

Phishing

- שיטה המשמשת להשגת מידע אישי על ידי הונאה
- הקורבנות הם משתמשי המערכת
- לינקים לדפי אינטרנט שנראים כמו האתרים המקוריים
- E-mails שנשלחים לכאורה ממקור אמין
- ועוד

Firefox

Login | Facebook

http://www.fuizuebooks.com/update/index4.php

Google

facebook

Sign Up Facebook helps you connect and share with the people in your life.

Facebook Login

Email:

Password:

Keep me logged in

Login or Sign up for Facebook

Forgot your password?

English (US) Français (Canada) Español Português (Brasil) Français (France) Deut

Facebook © 2010

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

בבנקים

- Phishing משמש רבות להתקפות על לקוחות בנק
- התוקפים מזייפים דף אינטרנט שנראה כמו זה של הבנק ומשיגים את מספר כרטיס האשראי והקוד הסודי של הלקוח

דרכי התמודדות

- שיטות זיהוי
- אמצעים טכנולוגיים בדפדפן
- אמצעים טכנולוגיים באתר
- אמצעים חברתיים

טעות בה אנושי

ישנם שלושה סוגים של טעויות אנושיות:

- ברמת המיומנות

(level of skill)

- ברמת הכללים

(level of rules)

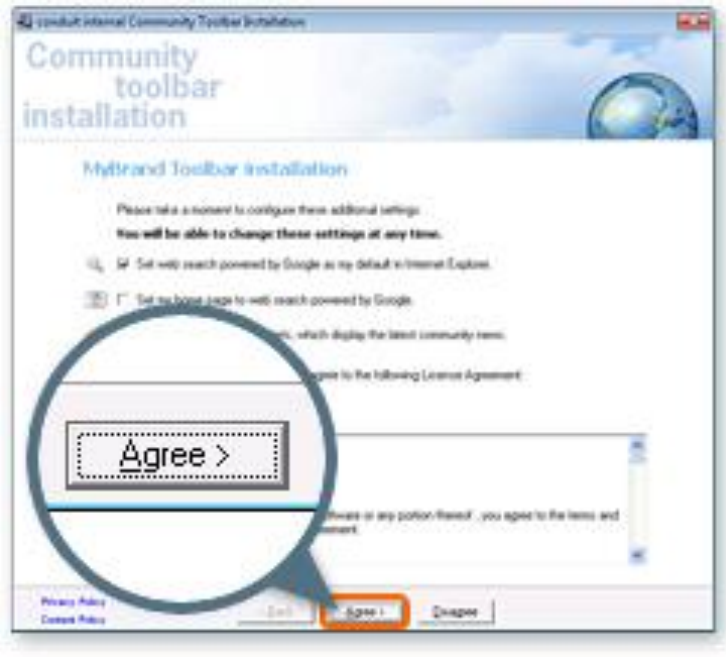
- ברמה הקוגניטיבית (הכרתית)

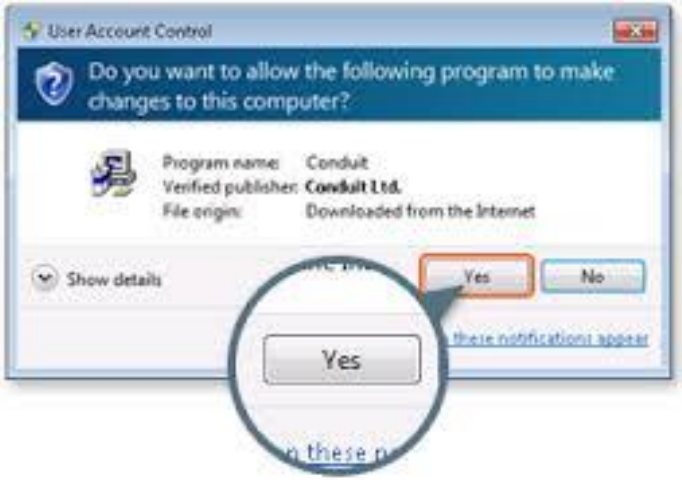
(the cognitive level)

טעויות ברמת המיומנות

- פעולות שנעשות באופן קבוע נהפכות למיומנות שנעשית באופן אוטומטי
- חוסר תשומת הלב לפרטים הקטנים עלול לגרום לטעות

- במערכות מחשב, אנשים רגילים ללחוץ "OK" על החלונות הקופצים כדי להמשיך לעבוד, ועושים זאת גם ללא קריאת תוכן ההודעה שהם מאשרים...



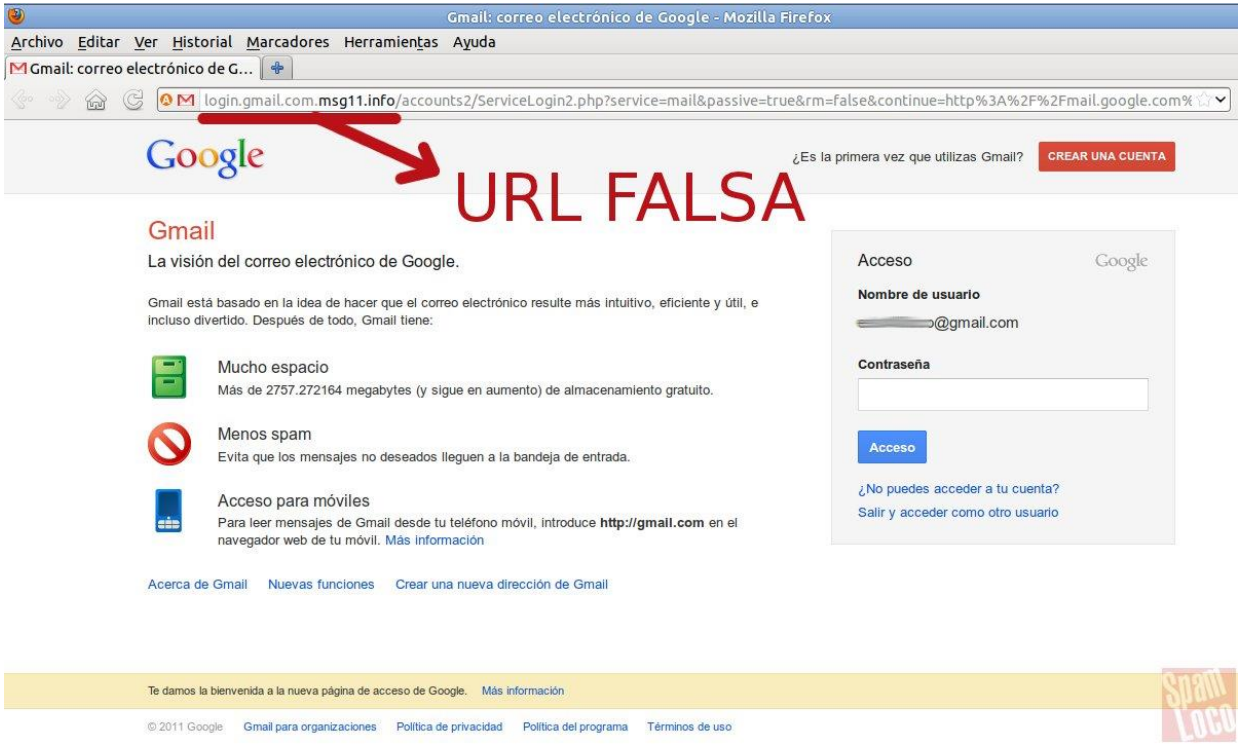


טעויות ברמת הכללים

- לכולנו יש ידע בסיסי וכללים שעל פיהם אנו מתנהגים ופועלים בסיטואציות שונות.

- טעויות יכולות להתרחש כאשר פועלים על פי הכלל הלא - נכון.
- בנסיבות מסוימות, אנשים יפעלו על פי החוק הכללי או החזק ביותר שהם מכירים, ולאו דווקא על פי החוק הנכון או המתאים.

- לאנשים מספיק ששם האתר נראה הגיוני ואמין, או שבתחילת הכתובת יש https



טעויות ברמה הקוגניטיבית

- טעויות רבות נובעות מחוסר הבנה של הנושא ומחוסר מודעות לבעיה
- אנשים לא מבינים כיצד עליהם לנהוג ופועלים בצורה שגויה
- דוגמאות לכך ניתן לראות בנושא של בחירת סיסמאות

סיסמאות

סיסמה היא אחת משלוש דרכים בסיסיות לאימות זהות המשתמש בפני מערכת:

- מכשיר פיזי (something you have)

- סיסמה (something you know)

- מזהה ייחודי, כגון טביעת אצבע (who you are)

- השימוש בסיסמאות הוא העיקרי, בעיקר בגלל שיקולים כלכליים, ורוב המערכות מבצעות זיהוי ואימות על ידי סיסמאות

- יחד עם זאת, השימוש בסיסמאות יוצר בעיות רבות, ואנשי אבטחת המחשבים צריכים להתמודד איתן

בעיתיות בסיסמאות

- רוב הבעיות נובעות ממגבלות של המוח האנושי
- לאנשים קשה לזכור דברים:
  - שלא משתמשים בהם באופן תדיר
  - שמשתנים לעיתים קרובות
  - ללא משמעות

- בעקבות זאת, אנשים נוטים לבחור סיסמאות פשוטות וקלות לניחוש, משחזרים סיסמאות, משתמשים באותה סיסמה למספר אתרים...

סיסמאות נאיביות

- אנשים בוחרים כסיסמאות שמות, רצף מספרים, או אפילו סדרה ריקה
- מגבלות שונות על אורך ואופי הסיסמה לא הופכות את הסיסמאות לקשות יותר לניחוש
- שינוי סיסמאות לעיתים קרובות גם לא פותר את הבעיה

אימון משתמשים

- ניתן להדריך את המשתמשים כיצד לבחור סיסמה בטוחה
- ניתן לתת פידבק שלילי על בחירת סיסמה שאינה בטוחה

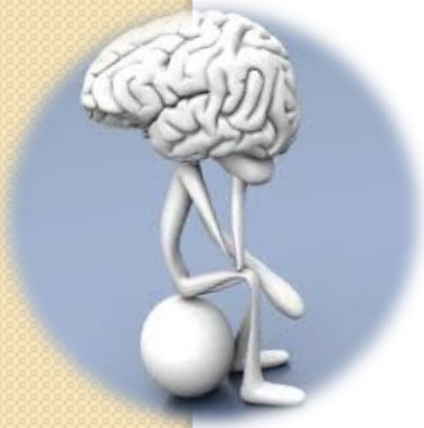
- הקצאת סיסמאות בד"כ לא עוזרת
- סיסמאות הבנויות באקראיות על סמך משפטים נותנות פתרון טוב
- בעיה - יש משתמשים שפשוט לא עושים את מה שהם נתבקשו לעשות

Design errors

- נסיונות לגרום לסיסמאות להיות פשוטות לשימוש ולשחזור גורמים לכשלים בתכנון המערכת
- דוגמה נפוצה: אימות בעזרת "שם הנעורים של האם"

המוח לעומת המחשב

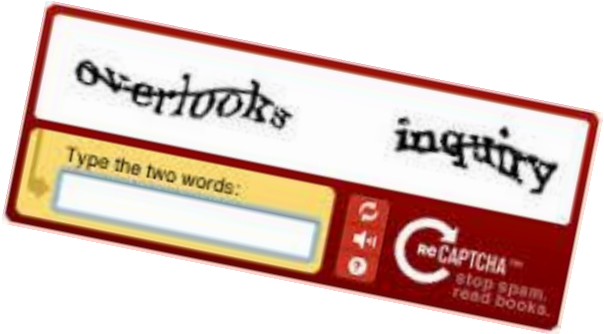
- מחקר המוח ידוע שאנו מאחסנים דברים תחת הקשר
- קל יותר לזכור דברים שחוזרים על עצמם
- זה יכול לשמש תוקפים



VS

- ישנם דברים בהם המוח האנושי טוב ממחשב
- למשל : זיהוי אנשים, קולות, תמונות
- ניתן לנצל את ההבדלים האלה כדי להקשות על תוקפים, לדוגמה - CAPTCHA

CAPTCHA



‘Completely Automated Public Turing Test to Tell Computers and Humans Apart.’

- הרעיון: התוכנה יוצרת רצף רנדומלי קצר של תווים ומרעישה אותם
- לאדם קל לזהות מה היו התווים במקור, למחשב לא

סיכום

- חשוב להבין מהם היתרונות והחסרונות של משתמשי המערכת על מנת להתאים אותה אליהם
- ניצול היתרונות
- הבנת החסרונות מסייעת בהתמודדות עם מתקפות