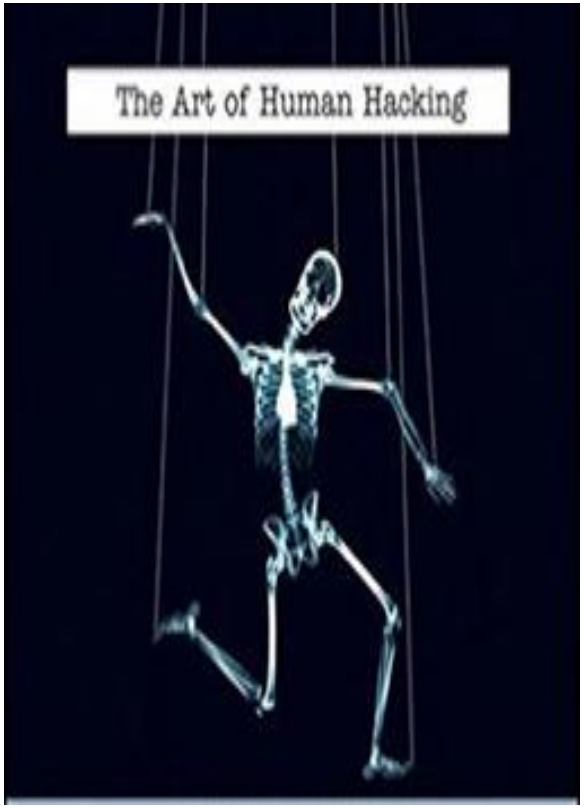
Usability & Psychology

Security Engineering

סמינר באבטחת מידע
מרצה: פרופ' אור דונקלמן
מוגש ע"י : נוהא דיאב

Social Engineering



- **הנדסה חברתית** - ניצול של תכונות פסיכולוגיות של האדם, אשר עשויות להביא אותו לציית לבקשותיו של הפורץ.
- למה תוקפים משתמשים ב SE ?
- מעשים זדוניים בהקשר של SE מאפשרים לעקוף את כל טכנולוגיות מנגנוני האבטחה.

https://images-na.ssl-images-amazon.com/images/I/41HpNgCrStL._SX332_BO1,204,203,200_.jpg

מתקפות פסיכולוגיות

- מכוון שהמשתמשים במחשב הם בני אדם, לחלק ניכר מהמתקפות העכשוויות היעד הינו בני אדם ולא מכונות.
- מתקפות אלו הולכות ומתגברות.
- לרוב, מתקפות דרך האינטרנט יותר קלות לבצוע וקשות יותר לעצירה.
- האנשים משתפרים ביכולתם הטכנולוגית.

Pretexting

- הגדרה – תקיפה ופריצה למערכת דרך האנשים שמפעילים אותה.
- להגדיר את עצמך כמישהו אחר על מנת לשלוף מידע פרטי.
- ההיבט הכי חשוב במתקפה זו הוא **אימון**.
- בד"כ חברות הן שסובלות מסוג זה של מתקפות, אך לאחרונה גם אנשים פרטיים מותקפים בשיטה זו.

http://www.social-engineer.org/framework/influencing-others/pretexting/

איך מתמודדים?

- לקבוע חוקים שמבטיחים העברה חסויה של מידע בין מפעילים.
- להסביר לאנשי הארגון את חשיבות החוקים שקיימים.

"Like any other defense to social engineering, you must be proactive and not reactive."

Phishing

- הוא ניסיון לגניבת מידע רגיש על ידי התחזות ברשת האינטרנט.
- פישינג מתבצע באמצעות התחזות לגורם לגיטימי המעוניין לקבל את המידע.
- בה הגורם המתחזה שולח קישור לאתר מזויף ומבקש מהקורבן להזין את פרטיו.
- בד"כ שולחים מייל שמכיל את הקישור.

מאת: <PayPal Inc. <support@inc.com
תאריך: 29 במרץ 2017 בשעה 12:32:42 GMT+3
אל: <wafakasis_geriatricdr@hotmail.com>
נושא: **Your account will be limited ! PayPal ID : PP-007-875-541-654**

https://support-noreply.kalyandrugs.com/redirection.php

PayPal

. Your account Will be limited

Dear Customer

- .juin 2016 We need to confirm some of your account information 07
- .Your case ID for this reason is PP-007-875-541-654
- . We face a problem in the ratification of the real owner of the account
- **:** And for that you must follow thefollowing steps

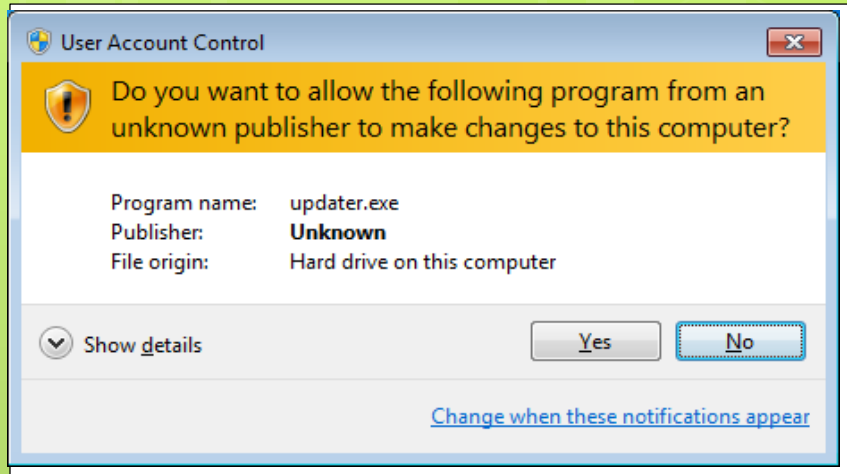
- **Click on the Get Started**
- **Log In Enter email and password**
- **Verify Your Informations To Activate Your Account**

Get Started

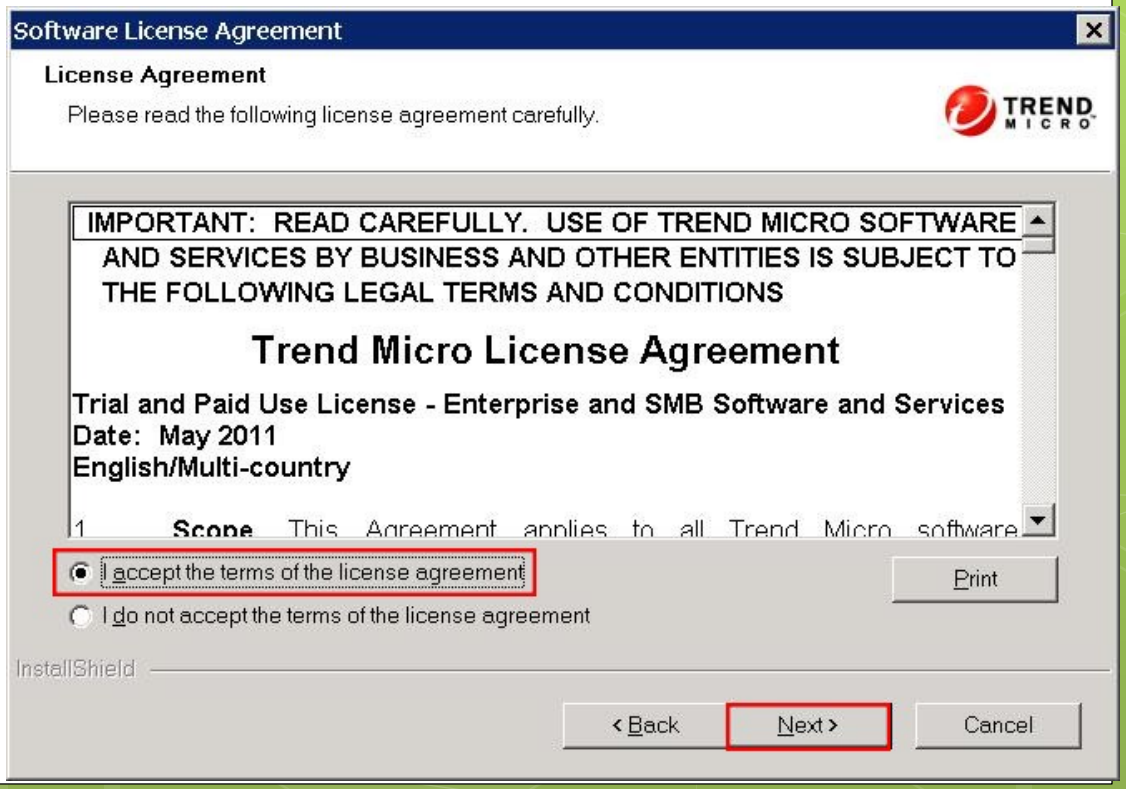
טעויות ברמת המיומנות

- פעולה שמתרגלים לעשותה באופן קבוע הופכת למיומנות שנעשית באופן אוטומטי.
- טעויות נגרמות מהעובדה שאנו רגילים לסיטואציות כלשהם ולא שמים לב לשינויים או לפרטים קטנים שגורמים לטעות.

http://patientsafetyed.duhs.duke.edu/module_e/types_errors.html



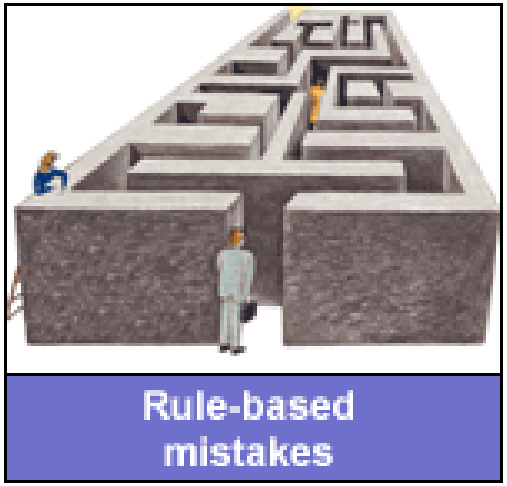
https://en.wikipedia.org/wiki/User_Account_Control



http://docs.trendmicro.com/en-us/enterprise/endpoint-application-control-20-sp1/installation/server-installation/license-agreement-sc.aspx

טעויות ברמת הכללים

- פעולות מתואמות כוונה , אך לא משיגות את התוצאה הנדרשת עקב יישום כלל באופן לא נכון או בחירה בכלל כללי יותר או חזק יותר מאשר הנכון.



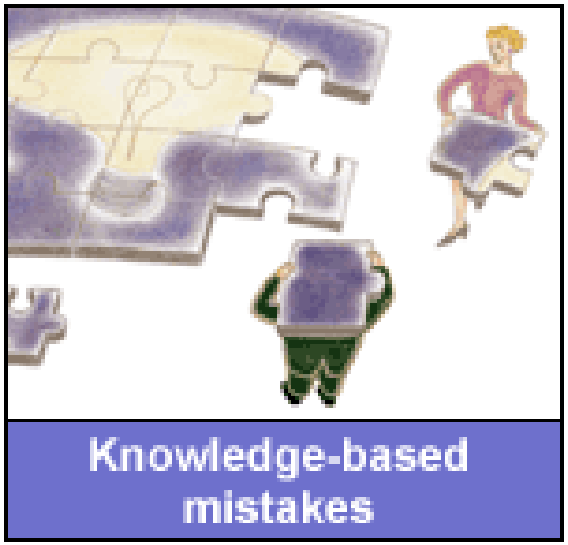
http://patientsafetyed.duhs.duke.edu/module_e/types_errors.html

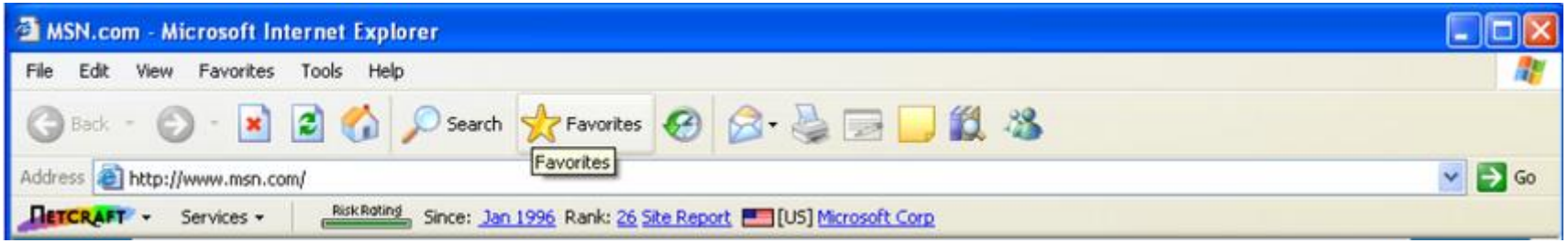
https://csiwodeadbodies.blogspot.co.il/2016/11/on-facebook-fake-news-and-election.html

http://www.silicon.co.uk/workspace/facebook-phishing-reporting-89000

טעויות ברמה הקוגניטיבית

- טעויות אלו נגרמות מחוסר ידע והבנה בנושא.





http://patientsafetyed.duhs.duke.edu/module_e/types_errors.html

https://www.researchgate.net/profile/Lorrie_Cranor/publication/221655330/figure/fig8/AS:305554208641037@1449861208773/Figure-8-The-Netcraft-Anti-Phishing-Toolbar-at-a-legitimate-web-site.png

Decision science

- מה הן היוריסטיקות וההטיות שבהם אנשים משתמשים כשמקבלים החלטות?
- תפיסת החברה לגבי סכנות.

https://blog.mailfence.com/wp-content/uploads/2015/11/human-nature-300x185.jpg

אימות משתמשים

- ישנם שלוש דרכים לאימות משתמשים במערכות:

1) something you have – מכשיר פיזי
2) something you know – סיסמה
3) Something you are – מזהה ייחודי

סיסמאות

בעיות השימוש בסיסמה:

א- האם המשתמש יזין את הסיסמה באופן תקין?

- סיסמה ארוכה או מסובכת מדי

ב- האם המשתמש יזכור את הסיסמה?

- ירשום אותה בצד
- סיסמה קלה\קשה לזכירה

ג- האם המשתמש יחשוף את הסיסמה שלו?

- בכוונה או בלי

בעיתיות בסיסמאות

מה לא כדאי לעשות:

- לבחור סיסמה שקשורה לשמך או לשמות בכללי
- שימוש באותה סיסמה למספר אתרים
- סיסמה קצרה וקלה מדי

מה לא בהכרח עוזר:

- מגבלות על אורך הסיסמה ותוכנה
- שינוי סיסמאות לעיתים קרובות

Top 25 most common passwords

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321
11. qwertyuiop
12. mynoob
13. 123321
14. 666666
15. 18atcskd2w
16. 7777777
17. 1q2w3e4r
18. 654321
19. 555555
20. 3rjs1la7qe
21. google
22. 1q2w3e4r5t
23. 123qwe
24. zxcvbnm
25. 1q2w3e

http://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/

http://www.backintheawesomedays.com/2014/01/creating-password.html

Please create a password

> *awesome*

Sorry, the password must be more than 8 characters

> *awesome day*

Sorry, the password must contain 1 numerical character

> *1 awesome day*

Sorry, the password cannot have blank spaces

> *25awesomedays*

Sorry, the password must contain at least one upper case character

> *25AWESOMEdays*

Sorry, the password cannot contain two consecutive upper case characters in a row

> *25AwesomeDaysPlease,IamGettingReallyFrustrated*

Sorry, the password cannot contain punctuation

> *LookHereYou*#$%*25AwesomeDaysAndImeanItThisTime*

Sorry, the password cannot contain special characters

> *Fine25AwesomeDaysPleaseThisIsTheLastTimeBeforeIthrowThisComputerOutTheWindow*

Sorry, that password is already in use!

https://memesuper.com/categories/view/12c98b5526e34ef967151e4e6da55d086179765c/password-meme.html

מה אפשר לעשות

- ללמד אנשים איך לבחור סיסמה בטוחה
  - בעיה – אנשים לא עושים מה שמבקשים מהם
- לתת משוב לגבי איכות הסיסמה
- לבחור סיסמה שבסיסה הוא משפט והיא מורכבת ממספרים ואותיות
  - יותר קל לזכור
  - קשות יותר לניחוש

סוגיות מערכת

סוגי התקפות על המערכת:

1. מתקפה מכוונת מטרה: התוקף מנסה לפרוץ רק לחשבון אחד מסוים.
2. פריצה לאיזשהו חשבון במערכת (ספציפית) , דוגמה קלאסית מתקפת פישינג על בנק.
3. פריצה לאיזשהו חשבון באיזשהי מערכת בדומיין מסויים.
4. מתקפה הכחשתית: התוקף רוצה למנוע משתמש חוקי מגישה למערכת.

עוד מתקפות

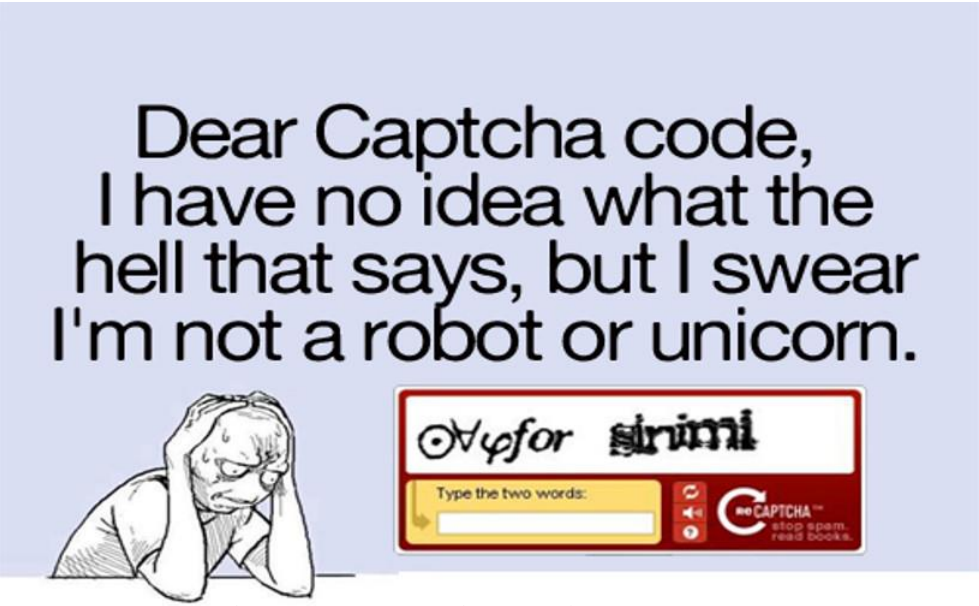
- רוב הזמן אזור הזנת הסיסמה אינו מוגן.
  - Interface design
  - Eavesdropping
  - PDP-10 TENEX
- מתקפות על אזור אחסון הסיסמאות.
  - השארת plaintext file לסיסמאות יכול להיות מסוכן.
  - Password cracking

Brain Vs. Computer

- מה המוח עושה יותר טוב ממחשב?
  - לזהות אנשים באופן ויזואלי
  - זיהוי תמונות בכללי
  - להבין נאום
  - לזהות מי המדבר
- כל מה שהוזכר לעיל אומר שיש אפשרות לבנות מבחנים שיזהו אם מדובר במחשב או בבן אדם.

CAPTCHAs

"Completely Automated Public Turing Test To Tell Computers and Humans Apart".



https://www.scienceabc.com/innovation/how-does-captcha-work-google-recaptcha.html

סיכום

- קל מאוד לרמות אנשים כי:
  - אנשים נוטים לתת אימון יתר באחרים.
  - בני אדם מכחישים את האיומים שמסביבם.

חיפוש בגוגל תמונות - denies

חיפוש בגוגל תמונות - trust

מקורות

- https://blog.mailfence.com/pretexting/
- http://www.social-engineer.org/framework/influencing-others/pretexting/
- https://he.wikipedia.org/wiki/%D7%94%D7%A0%D7%93%D7%A1%D7%94_%D7%97%D7%91%D7%A8%D7%AA%D7%99%D7%AA_(%D7%90%D7%91%D7%98%D7%97%D7%AA_%D7%9E%D7%99%D7%93%D7%A2)