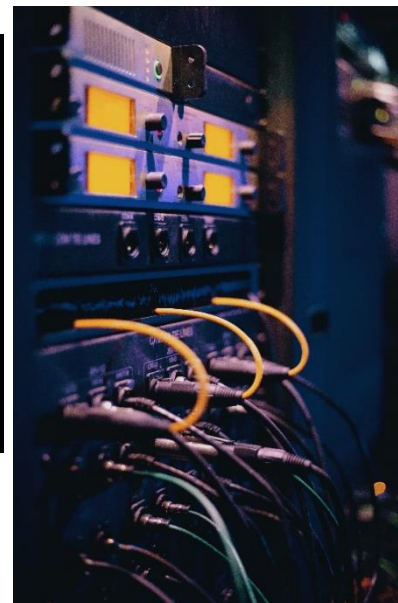


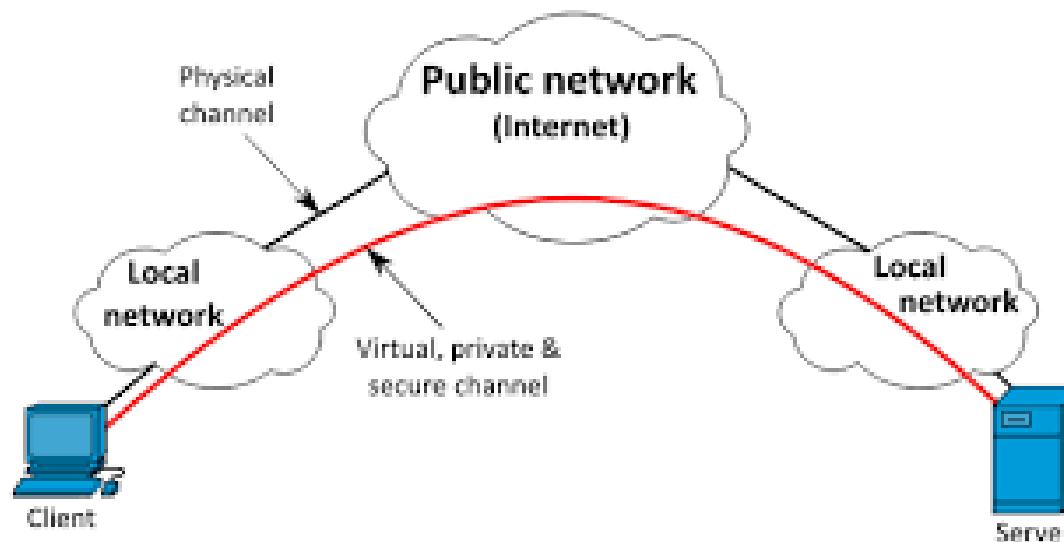
מושגי ייסוד בסייבר – חלק ב



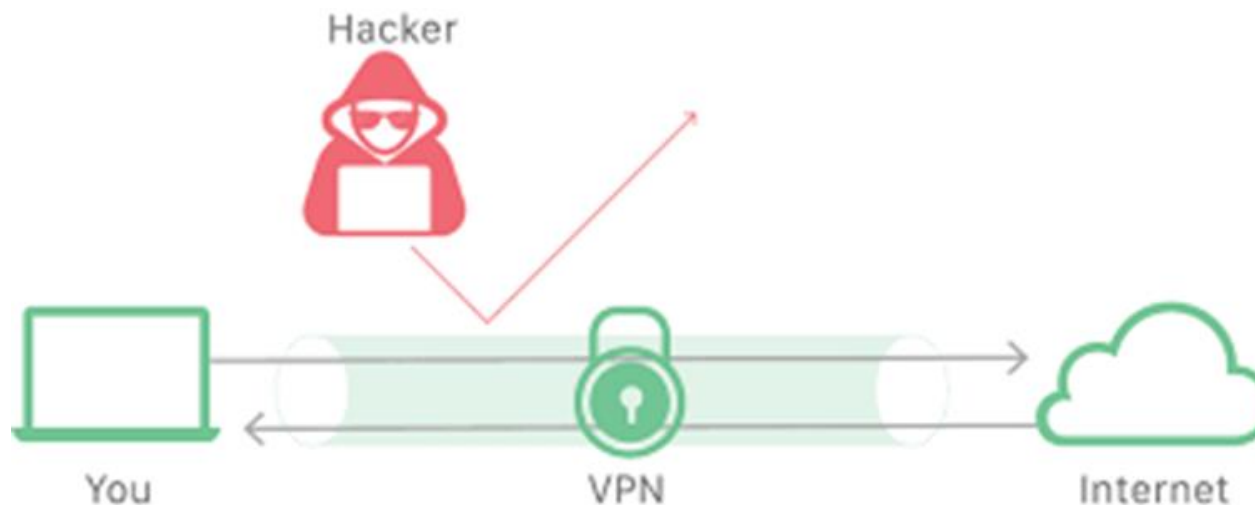
תקשורת אל הארגון - באמצעות VPN

data authorized network
security encryption
virtual private network
VPN tunnel
anonymous VPN private
internal network authenticate privacy Internet

VPN = VIRTUAL PRIVATE NETWORK

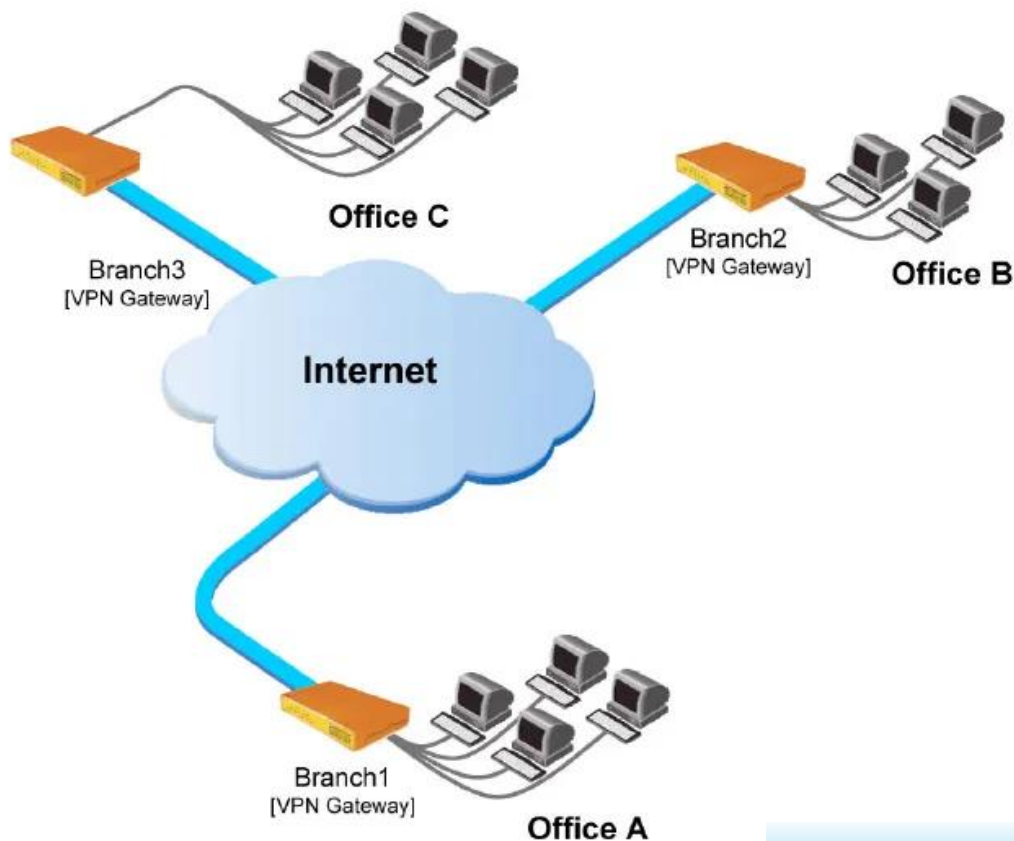


תקשורת עוברת בצינור (TUNNEL) מוצפן



תקשורת אל הארגון - באמצעות VPN - שימושים

Kuku Japan

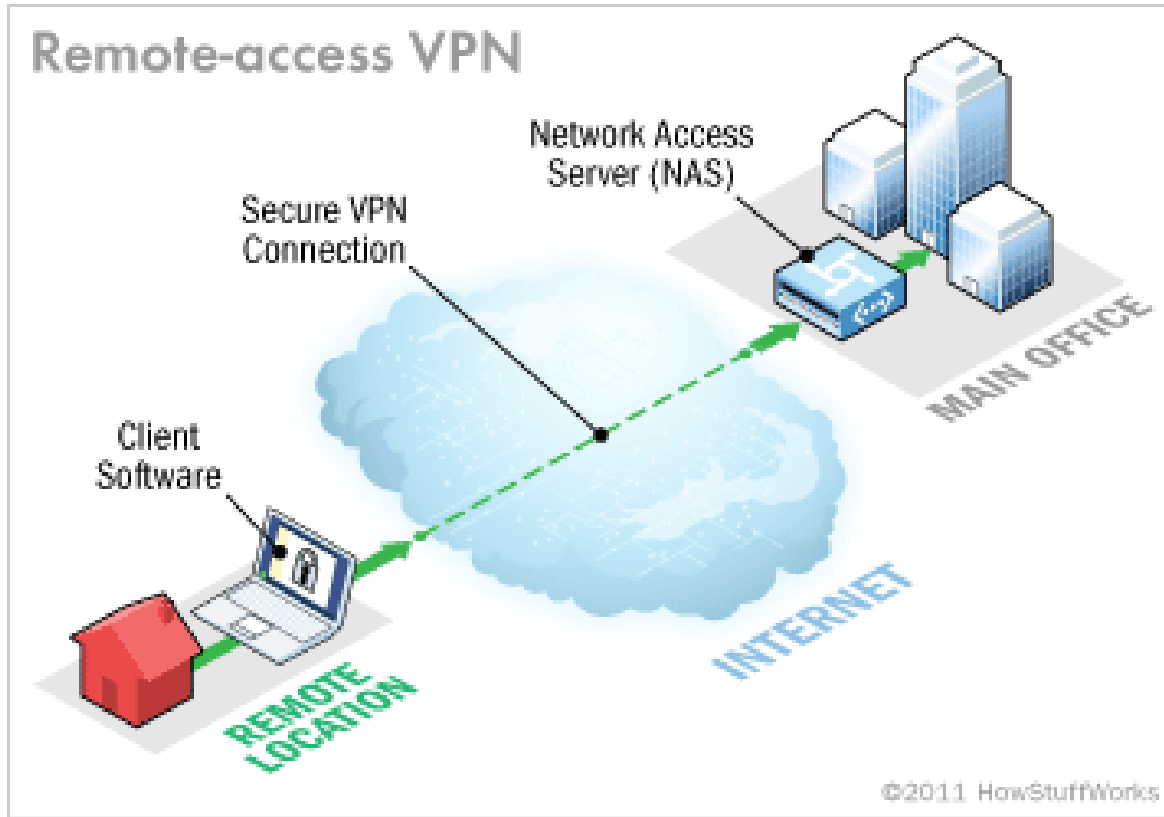


ארגון מפורז על פני שטח גיאוגרפי גדול

Kuku ISRAEL

Kuku U.S.A

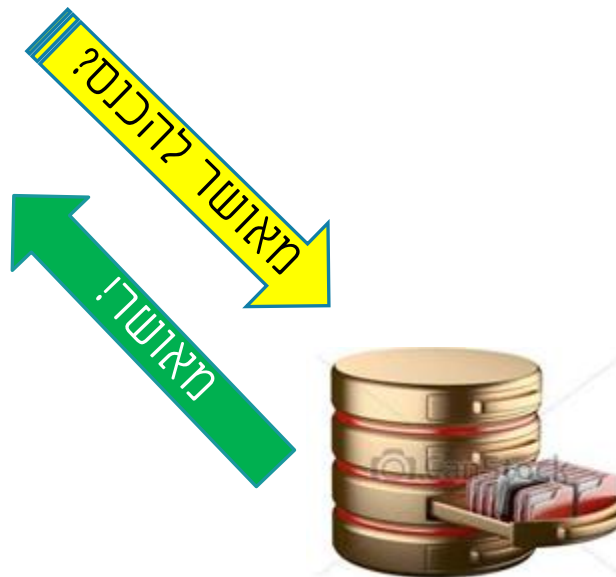
גישה מרחוק של משתמשים



הזדהות למערכת - איך עובדת סיסמא?



שם משתמש: Hr105
 סיסמא: 123456



איך עובדת הזדהות?

שם משתמש	סיסמא	סטטוס אישור
Uv451	123123	
Db633	11qq11	
Hr105	123456	
tp423	password	✓
-----	-----	
-----	-----	

סיסמאות נפוצות

208 הסיסמאות הנפוצות לפי נתונים שנאספו על ידי פורצים טורקיים רוב הסיסמאות נאספו, ככל הנראה, מהומלס ומפיצה האט, יש לא מעט סיסמאות שקשורות לשני האתרים האלה. המידע מבוסס על סט של כ-110,000 סיסמאות.

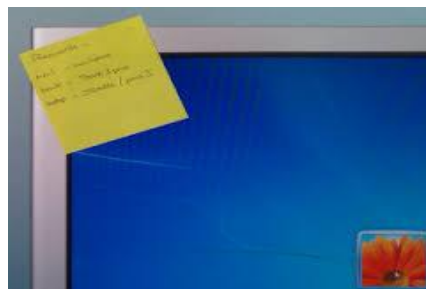
מספר סידורי	סיסמה	מופעים
1	123456	2419
2	1234	1875
3	12345	1115
4	12345678	445
5	123123	218
6	1111	216
7	qazwsx	189
8	1234567	164
9	0	155
10	123	154
11	121212	152
12	1212	139
13	111111	122
14	55555	109
15	pizza	100

הבעיה:
שימוש בסיסמאות חלשות

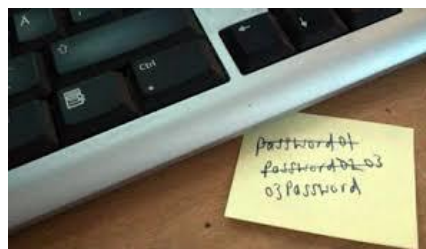
בעיות עם סיסמאות



➤ סיסמא קלה



➤ ואם מאלצים סיסמא לא קלה.....
תולים על מסך המחשב



➤ שמים מתחת למקלדת

יש לזכור: קיימות טכנולוגיות BRUTE FORCE וטכנולוגיות DICTIONARY מתקדמות לזיהוי סיסמאות ברשת

פתרון:

- ✓ רצוי מאד 8 תווים אך לא פחות מ- 6 תווים
- ✓ מורכבות סיסמא (אות גדולה, קטנה, מספר, תו מיוחד) 3 מתוך ה-4

דוגמאות לסיסמאות שקל לזכור וקשה לפרוץ:



1. P@55w0rd

2. Pשדד'סרג

מהירות הפריצה לסיסמא קלה

(96⁸)

P@55w0rd

26⁸

password

Test a New Password

Enter in a password to see the maximum time it would take to crack that password. Use the slider under the year to see how much the maximum crack time has increased since 1982. Also slide up to 2020 to see how quickly a password might be cracked in the future.

Password: P@55w0rd Year: 2020

9 YEARS, **6** MONTHS, **2** WEEKS, **4** DAYS, **5** HOURS, **54** MINUTES, **32** SECONDS, **79** JIFFIES, **8** MILLISECONDS

Keys per second in 2020: 17042497.3 kps Word List: On Off

This interactive is not collecting entered passwords and is for entertainment purposes. Estimates made in the interactive will not always be accurate due to evolving technologies and limitations in technology used to create it.

Better Buys

Test a New Password

Enter in a password to see the maximum time it would take to crack that password. Use the slider under the year to see how much the maximum crack time has increased since 1982. Also slide up to 2020 to see how quickly a password might be cracked in the future.

Password: password Year: 2020

0.19 MILLISECONDS

Keys per second in 2020: 17042497.3 kps Word List: On Off

This interactive is not collecting entered passwords and is for entertainment purposes. Estimates made in the interactive will not always be accurate due to evolving technologies and limitations in technology used to create it.

Better Buys

<https://www.betterbuys.com/estimating-password-cracking-times/#:~:text=Nine%2Dcharacter%20passwords%20take%20five,bad%20for%20one%20little%20letter.>

מהירות הפריצה לסיסמאות

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %\$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

דאגו שהסיסמה תהיה באורך של 8 תווים לפחות ותכלול:

- שילוב של אותיות קטנות וגדולות (a-z, A-Z)
- ספרה אחת לפחות (0-9)
- תו מיוחד אחד לפחות (\$,%,&,@)

השאירו את פרטיכם האישיים ופרטים אודותיכם מחוץ לסיסמה.

שמות משמעותיים: שקלו להשתמש בהקשר - אם מדובר בניח בחשבון מקוון, חישוב על מילה המתקשרת אליו. למשל: אפשר לקשר את הסיסמה של חשבון הבנק, לשם הרחוב שבו הסיניף מתנהל בהתחשבות בהמלצות ה"ל".

זכרו: שימוש בתו "רווח" יכול לעזור בהגנת הסיסמה.

קחו משפט שלם וארוך שיהיה לכם קל לזכור והפכו אותו לראשי תיבות. למשל My dog's name is Mooshi. הסיסמה תהיה: MdniM. לאחר הוספת ספרה ותו מיוחד, הסיסמה תהיה: MdniM1!

במידה ואורך הסיסמה מאפשר זאת, שיקלו להשתמש ב Passphrases כסיסמתכם - הנה סיסמה המורכבת ממשפט או מחיבור של כמה מילים:

שקלו להשתמש במחרוזת קבועה - כמו ביטוי, מילים משי, ציטוט מסרט ולהוסיף לה סימנים ותווים מיוחדים, למשל Wish1You@WereHere!

עוד אפשרות הנה סיסמה המבוססת על תרגיל חשבון פשוט עם שילוב מילים במקום ספרות. לדוגמה, הסיסמה 3 Hundred - 3 =297

כיצד בונים סיסמא חזקה?

מקור: באדיבות משרד הבריאות

הפתרון: הזדהות חזקה (MFA)



הזדהות ב-2 רמות (2 Factor Authentication)

הזדהות ב-3 רמות (3 Factor Authentication)

רמה I – משהו שאתה יודע – **Something you know**

רמה II – משהו שיש לך – **Something you have**

רמה III – משהו בך – **Something you are**

הזדהות ברמה שניה- משהו שיש לך (פיסית)



➤ מכשיר סלולרי – קבלת SMS



➤ טוקן ייעודי



➤ כרטיס חכם

הזדהות ברמה שלישית - משהו בך (ביולוגית)



טביעת אצבע ✓

זיהוי רשתית ✓

תווי פנים ✓

זיהוי קולי ✓

מאפייני התנהגות ✓

סרטון בנושא 2 FACTOR





תקיפות סייבר



התקפות סייבר ב-2021



- היקף ההתקפות על ארגונים/חברות בעולם עלה בשנת 2021 בכ-50%.
- ברבעון 4 עמד מספר התקיפות הממוצע בעולם, פר ארגון/חברה, על יותר ל-900 מתקפות בשבוע.
- הסקטורים המותקפים ביותר בעולם היו : חינוך ומחקר (1,605 מתקפות פר ארגון בשבוע), ממשל/צבא (1,136 מתקפות פר ארגון בשבוע) ותקשורת (טלקומוניקציה – 1,079 מתקפות פר ארגון בשבוע).
- מבחינה גיאוגרפית, האזור עם היקף המתקפות השבועי, פר ארגון, הגדול ביותר בעולם היה אסיה-פסיפיק (1,353 מתקפות פר ארגון בשבוע), לאחר מכן דרום אמריקה (1,118 מתקפות פר שבוע), אירופה (670 מתקפות פר ארגון בשבוע) וצפון אמריקה (503 מתקפות פר ארגון בשבוע).

סקר מערך הסייבר הלאומי והלמ"ס

המדגם כלל כ-2,500 עסקים

- שניים מכל חמישה עסקים גדולים חווה תקיפת סייבר (42%)
- בקרב תעשיית טכנולוגיית עילית (47%)
- בענפי ההיי-טק, אחד מכל שלוש חברות דיווחו על תקיפה (37%)
- כ-15% מהעסקים הקטנים חוו מתקפת סייבר

חדשות

אחד מחמישה עסקים בישראל חווה תקיפת סייבר

תאריך פרסום: 21.07.2021

אחד מכל חמישה עסקים בישראל (18%) חווה תקיפת סייבר - כך עולה מסקר חדש של הלמ"ס ומערך הסייבר הלאומי

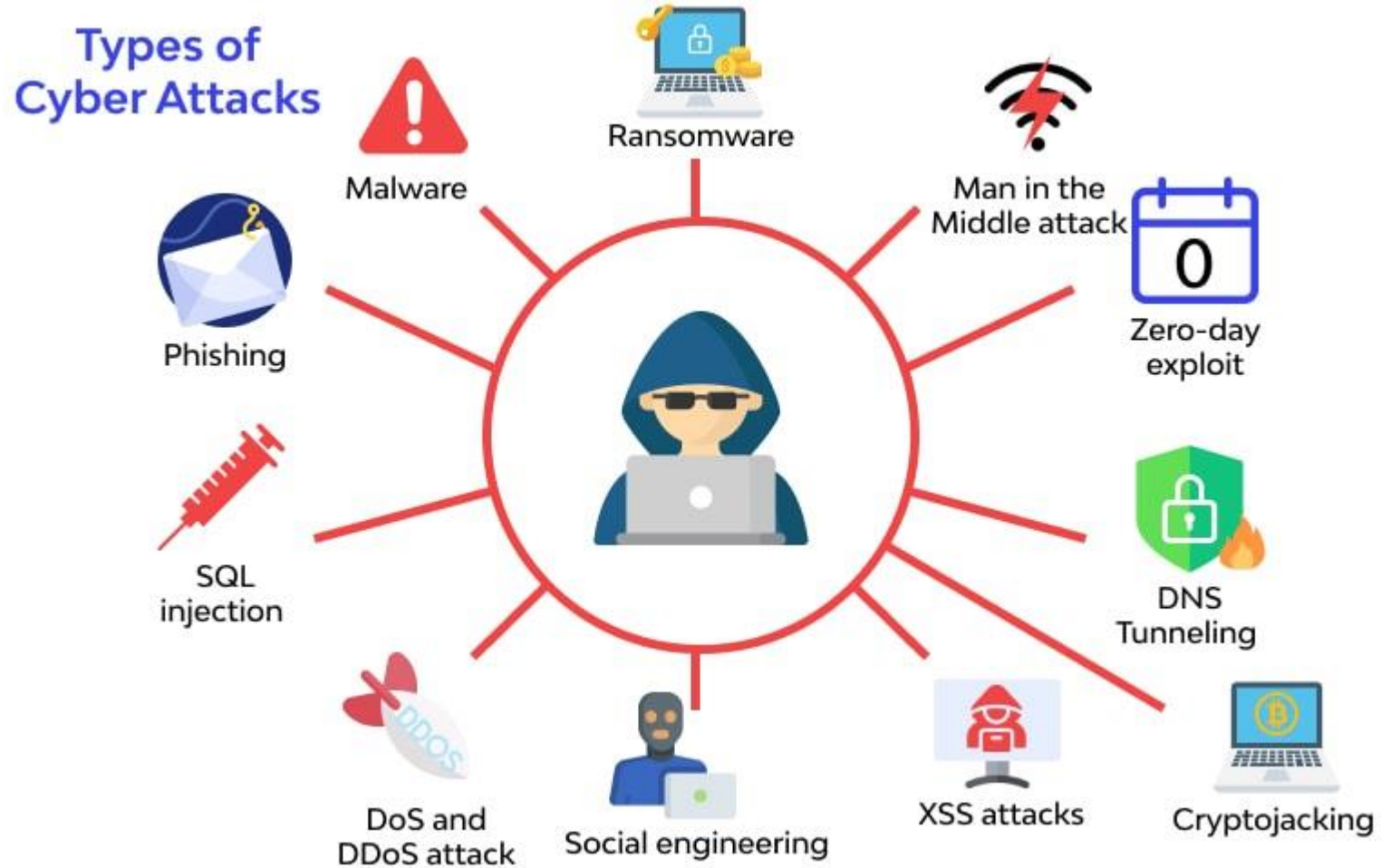


שתפו:

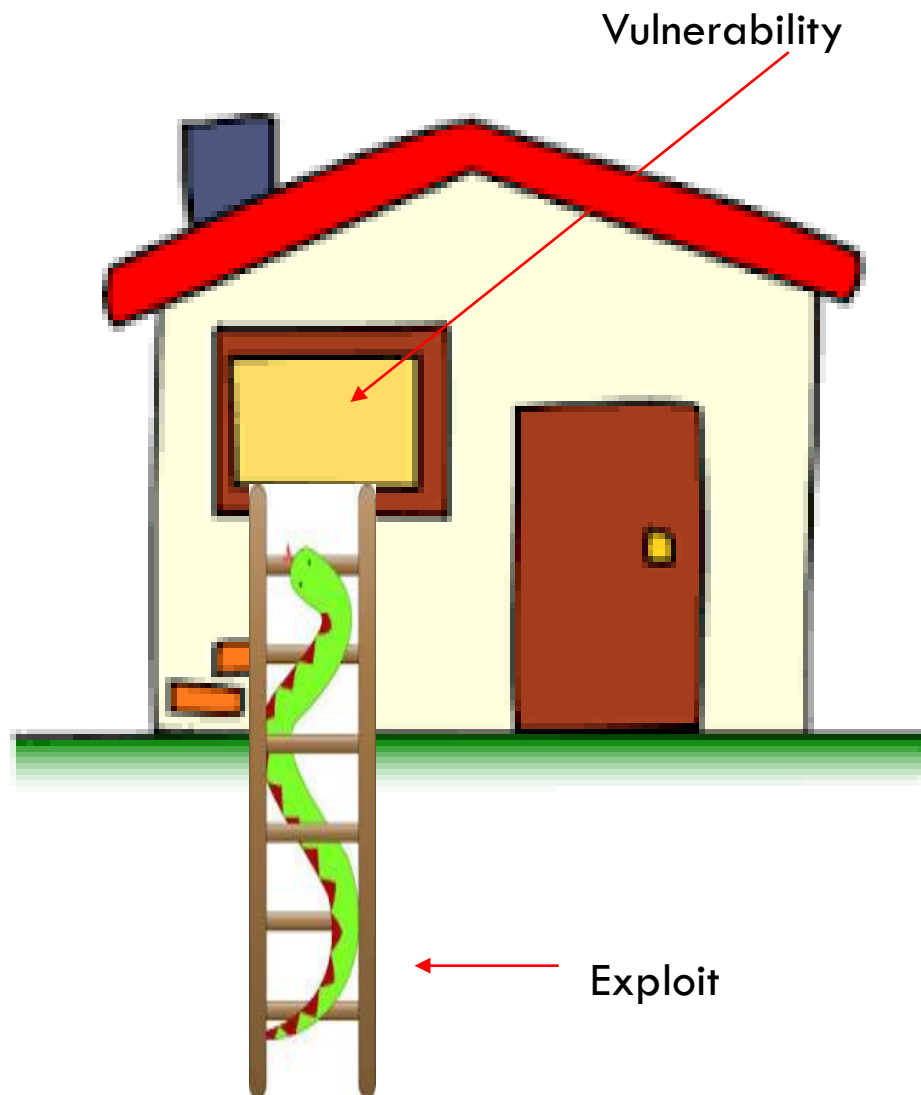


<https://www.gov.il/he/departments/news/cyberweeknews>

סוגי התקפות



התקפה על האפליקציה



Vulnerability – חולשה □

Exploit – ניצול חולשה □

אנלוגיה לעולם המיחשוב:

חולשה: באג בתוכנת דפדפן אקספלורר של מיקרוסופט המאפשר פריצה אל המחשב שלנו

ניצול החולשה: תוכנות שהאקרים כתבו ופרסמו באינטרנט על מנת ל"התנקם" בחברת מיקרוסופט

מי מנצל: כל מי שמוריד את התכנה

התקפת DOS , DDOS



התקפת Denial of Service – DOS

התקפת Distributed Denial of Service – DDOS

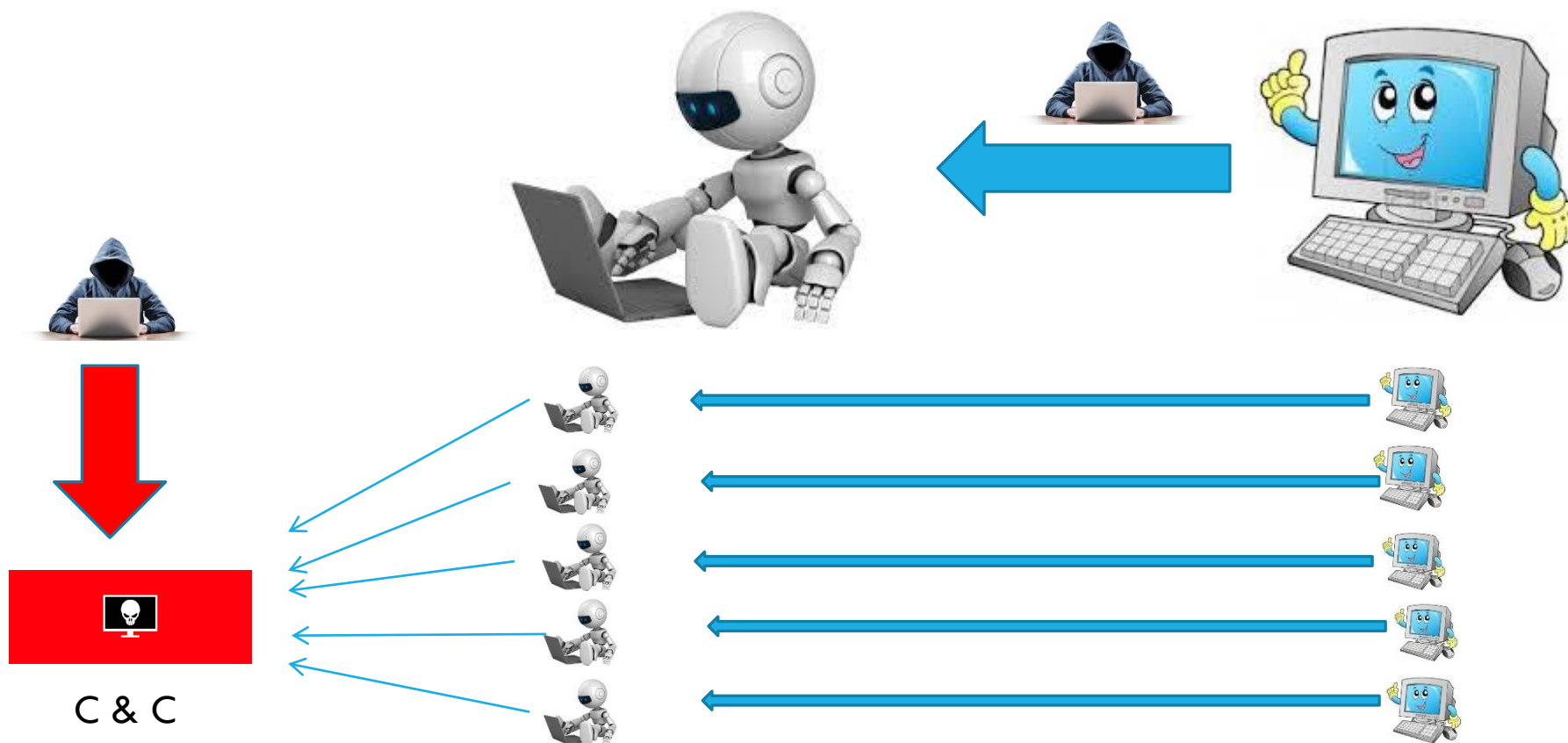
הרכיבים המעורבים:

- אתר אינטרנט כלשהו שנפרץ (למשל hotels.com)
- מחשב הקורבן שהופך לבוט
- מחשב התוקף
- תחנת ניהול הבוטים שמקים התוקף

בוט – מחשב שנמצא תחת שליטה חסויה של האקר

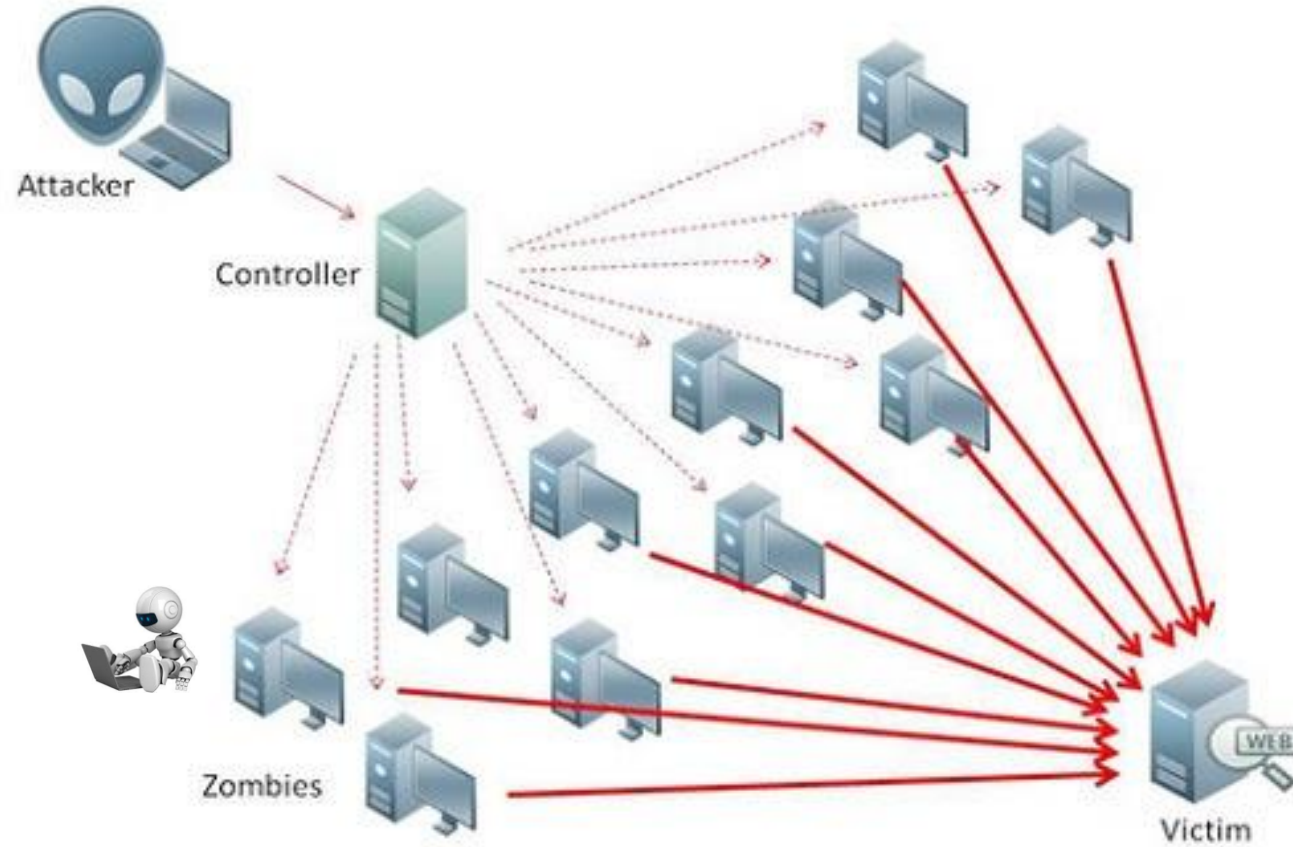
שלבי ההתקפה בהתקפת DOS

התוקף הופך מחשב ל-BOT





ביצוע ההתקפה



אפשר גם לקנות התקפות מוכנות באינטרנט

<http://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html>

How much costs a DDoS attack service? Which factors influence the final price?

March 26, 2017 By [Pierluigi Paganini](#)

How much costs a DDoS attack service? Kaspersky Lab published an analysis on the cost of a DDoS attack and services available in the black markets.

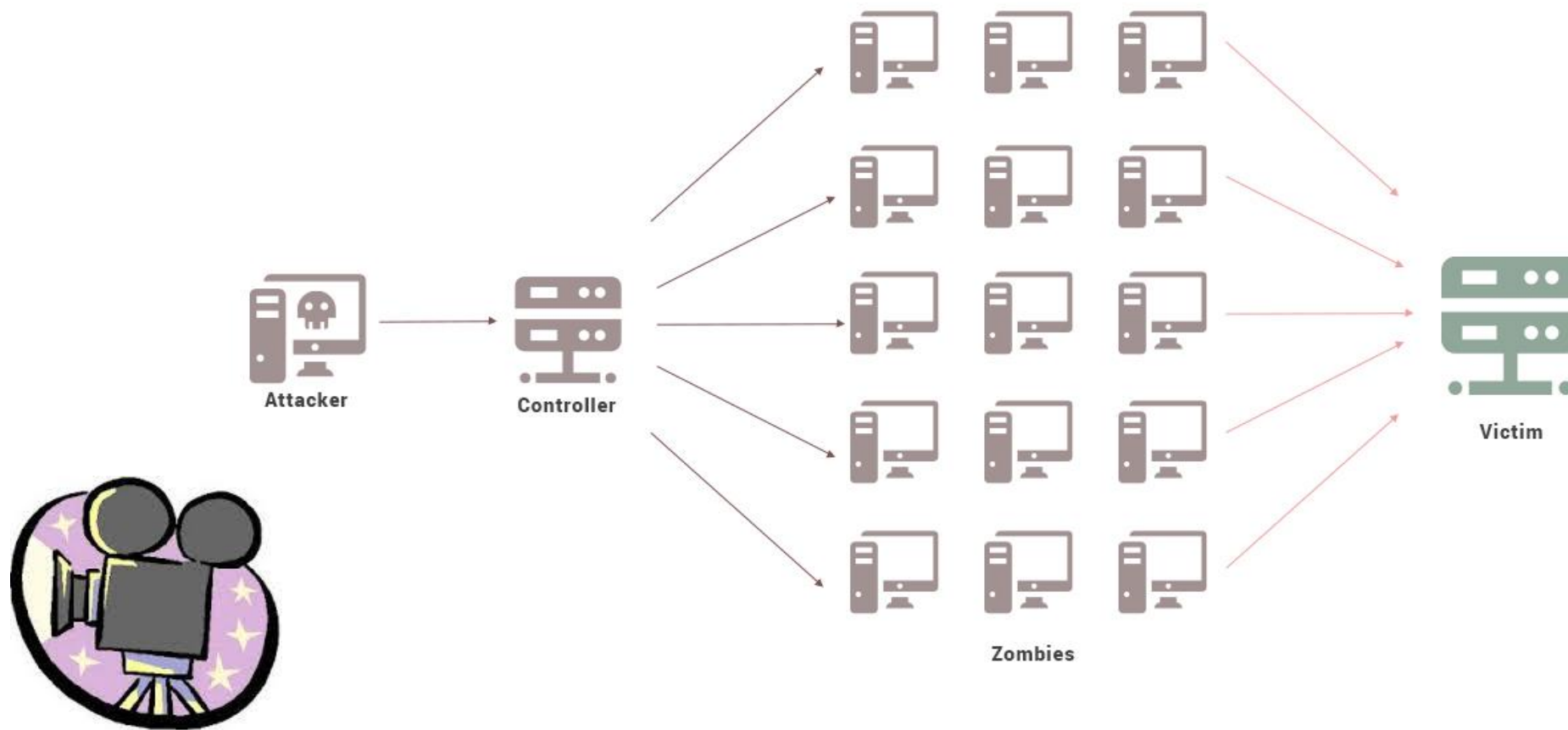
Kaspersky Lab has published an interesting analysis on the cost of DDoS attacks. The experts estimated that the cost to power a DDoS attack using a **cloud-based botnet of 1,000 desktops is about \$7 per hour**. A DDoS attack service typically goes for \$25 an hour, this means that the expected profit for crooks is around $\$25 - \$7 = \$18$ per hour.

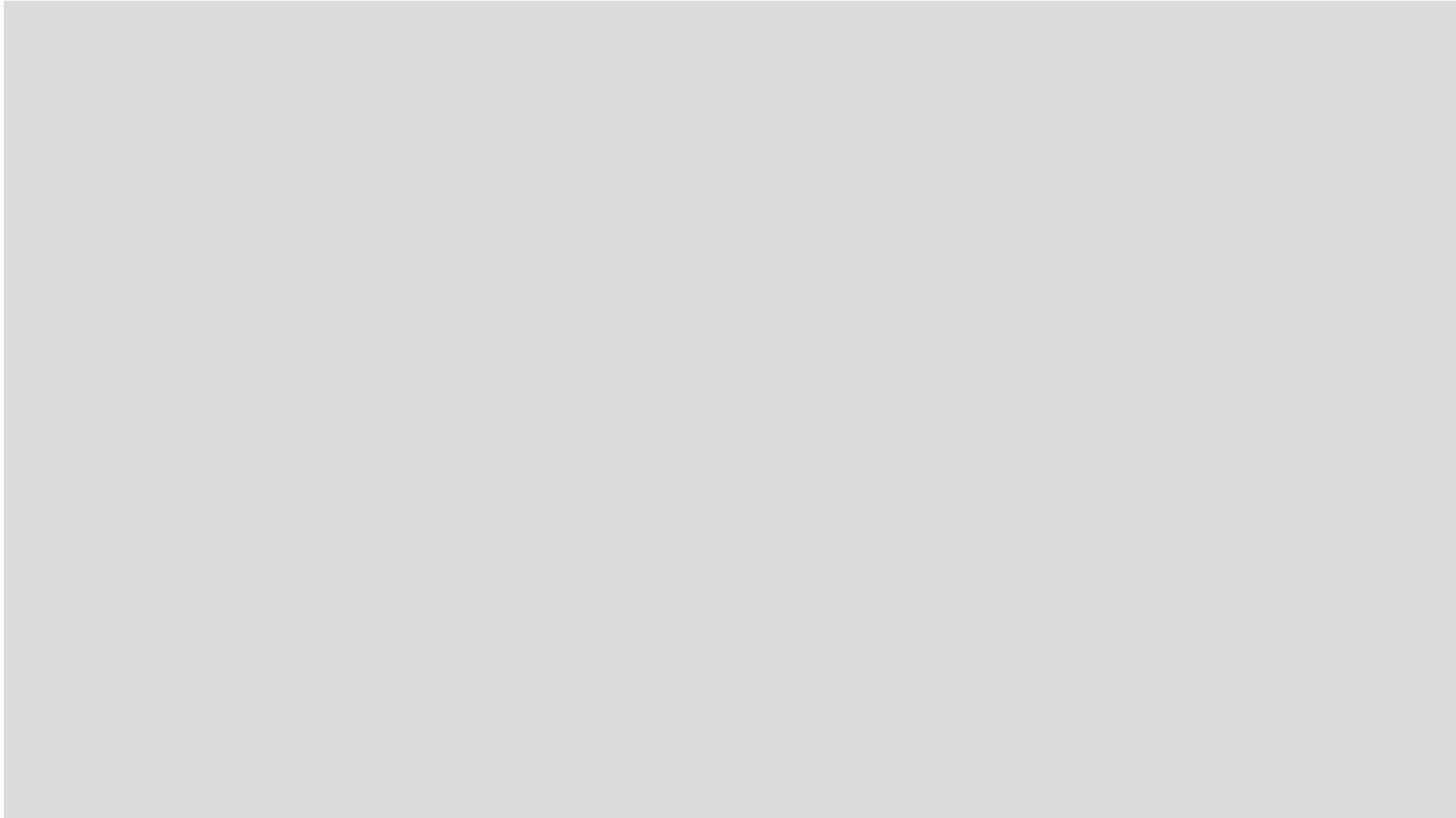
Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

התקפת DDOS - סרטון

התקפת DDOS - סרטון





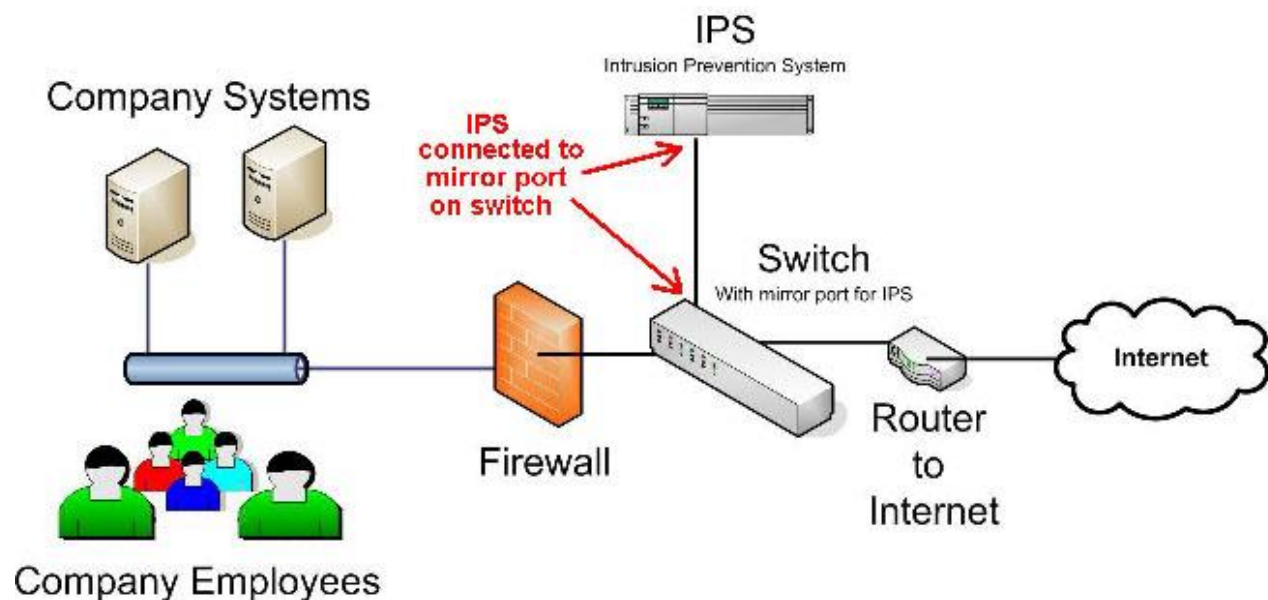
IDS , IPS - הגנה כנגד התקפות

IDS = INTRUDER DETECTION SERVICE

IPS = INTRUDER PROTECTION SERVICE

IDS - במקרה של התקפה על הארגון - מתריע בלבד

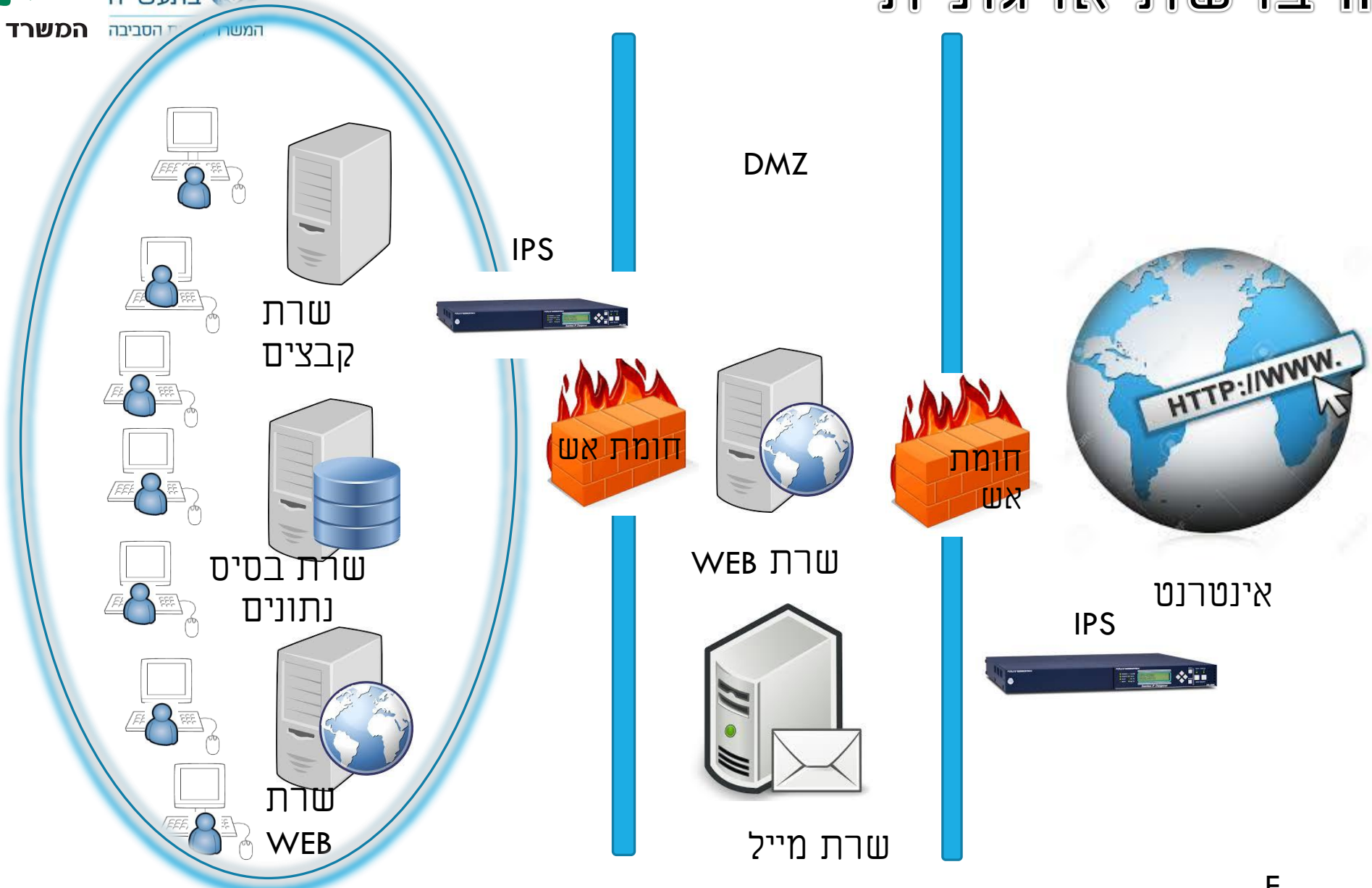
IPS - מתפקד כ-IDS ובמידת הצורך, אם קינפגנו אותו כך - יכול לחסום התקפות בצורה אקטיבית



הצורך:

- חסימת התקפות מחוץ לארגון
- חסימת התקפות מתוך הארגון

מיקום IPS ברשת ארגונית



בעיות בחסימת התקפות

ב-IPS יש לקחת בחשבון **חסימת תעבורה לגיטימית***

מצב חסימה	סוג התעבורה	מצב
מאפשר	לגיטימית	1
1 בעיה חוסם	לגיטימית	2
2 בעיה מאפשר	לא לגיטימית (התקפה)	3
חוסם	לא לגיטימית (התקפה)	4

מי יותר גרוע לארגון ??

בעיה 1 או בעיה 2?

בעיות בחסימת התקפות במערכת IPS



בעולם ה-זו – השבתת גישה למערכת מידע



בעולם ה-זס – פס ייצור **מושבת!!**

איך להתגבר על החסרון? הפעלת IDS ולאחר קבלת התראה שיקול דעת אנושי מה לחסום בפועל



מה זה וירוס?

וירוס זה תוכנה העשויה מקוד מסוים שהיא בתוך קובץ הרצה מסוים ויש לו יכולות שכפול.

2 סוגים עיקריים:

- ❑ וירוס אקטיבי-וירוס שעובר ממחשב למחשב
- ❑ וירוס פאסיבי-שנשאר רק במחשב אחד.

פעולות לדוגמא שמבצעים וירוסים:

- ❖ וירוס שיכול למחוק את הקבצים במחשב או לשנות אותם
- ❖ וירוס ששולח מידע מהמחשב לעמדת הבקרה של ההאקר
- ❖ וירוס שמאפשר שליטה מרחוק על המחשב

1. תולעים

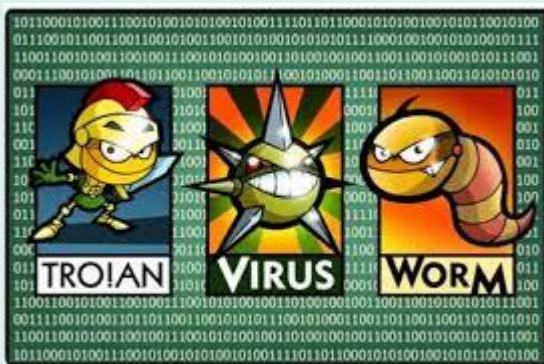
התולעים פועלים באופן עצמאי ומטרתם העיקרית היא להתפשט בכל המחשב ולהביא לקריסתו התולעת משכפלת מפיצה את עצמה ממחשב ומגיעה לנפחים אדירים.

2. סוס טרויאני

סוס טרויאני הוא תוכנה שיכולה לשנות קבצים או למחוק אותם או לגנוב באמצעות שליטה מרחוק ע"י מחשב מרוחק.

3. פצצות לוגיות

פצצות לוגית היא וירוס שפועל ע"פ תאריך/יום/שעה. הפצצה הלוגית עושה פעולה כלשהי שגורמת נזק למחשב.



4. תוכנת רוגלה (SPYWARE)

זוהי תוכנה אשר מסוגלת להציג למישהו במחשב מרוחק מידע על המחשב שתוכנה זו נכנסה אליו. בניגוד לסוס טרויאני, תוכנה זו לא מסוגלת לשנות או למחוק קבצים.



5. וירוסי מאקרו

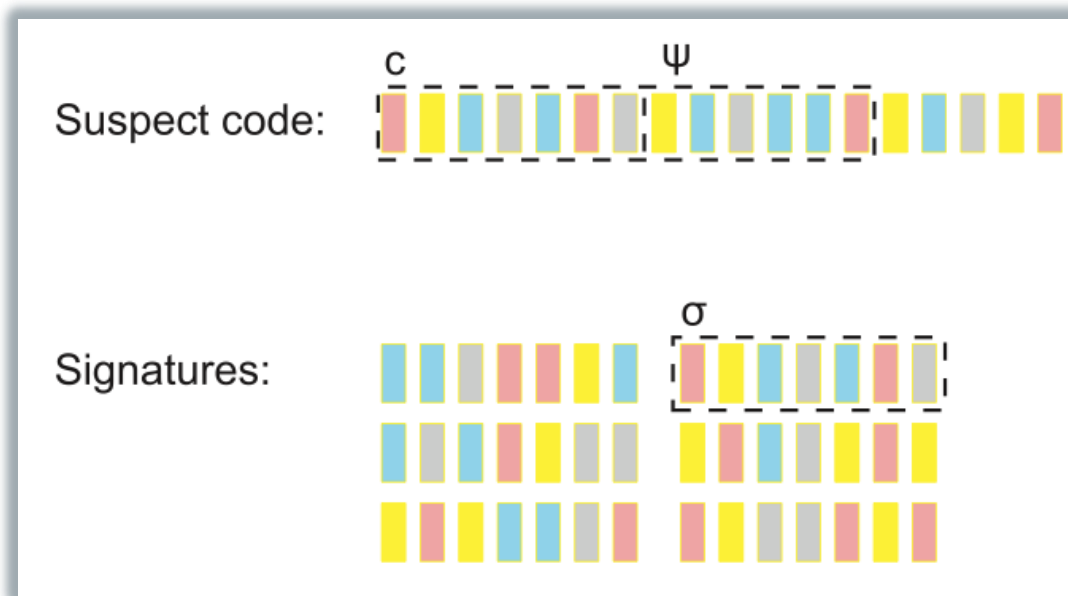
וירוסים אלו מתחבאים בתוך מסמכים סטנדרטיים כמו וורד או אקסל. וירוסים אלו יכולים לגרום למחיקת קבצים או הרס מערכת ההפעלה

איזה סוג של וירוס לא הזכרנו כאן ?? !!!



איך מתגוננים ?

חברות אבטחת מידע מייצרות חתימות לוירוסים הידועים



חתימות:

מה החסרונות: מוגנים בפני וירוסים ידועים בלבד

ZERO DAY



מהו וירוס ZERO DAY?



וירוס לא ידוע לחברות האנטי וירוס ולכן לא מופיע בקובץ החתימות של האנטי וירוס המותקן במחשבינו.

איך מייצרים וירוס ZERO DAY ?

2 אפשרויות:

1. יוצרים וירוס חדש לגמרי שלא מוכר עדיין (לכן נקרא ZERO DAY כי זה היום הראשון שלו בחוץ)

2. לוקחים וירוס קיים ויוצרים ממנו "מוטציה" לעיתים מזוהה ע"י קובץ החתימות של ה-AV ולעיתים לא

דוגמאות ל-ZERO DAY

וירוסי כופרה שונים



CryptoLocker **Your Personal files are encrypted!** English

Support e-mails: supteam03@india.com supteam03@yandex.ru

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique public key RSA-2048 generated for this computer.**

To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that **nobody and never** will be able to **restore files.**

To obtain the private key for this computer, which will automatically decrypt files, you need **pay 0.55 Bitcoin (~386 USD)**

You can easily delete this software, but you must know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click 'Pay with Bitcoin'. To open a list of encoded files, click 'Show Files'.

Do not delete this list, it will be used for decryption. And do not move your files.

Private key will be destroyed on
11/12/2016 6:07:01 PM

Time left
119:54:00

Received: **0.00 BTC**
Checking wallet..

Show files Pay with Bitcoin

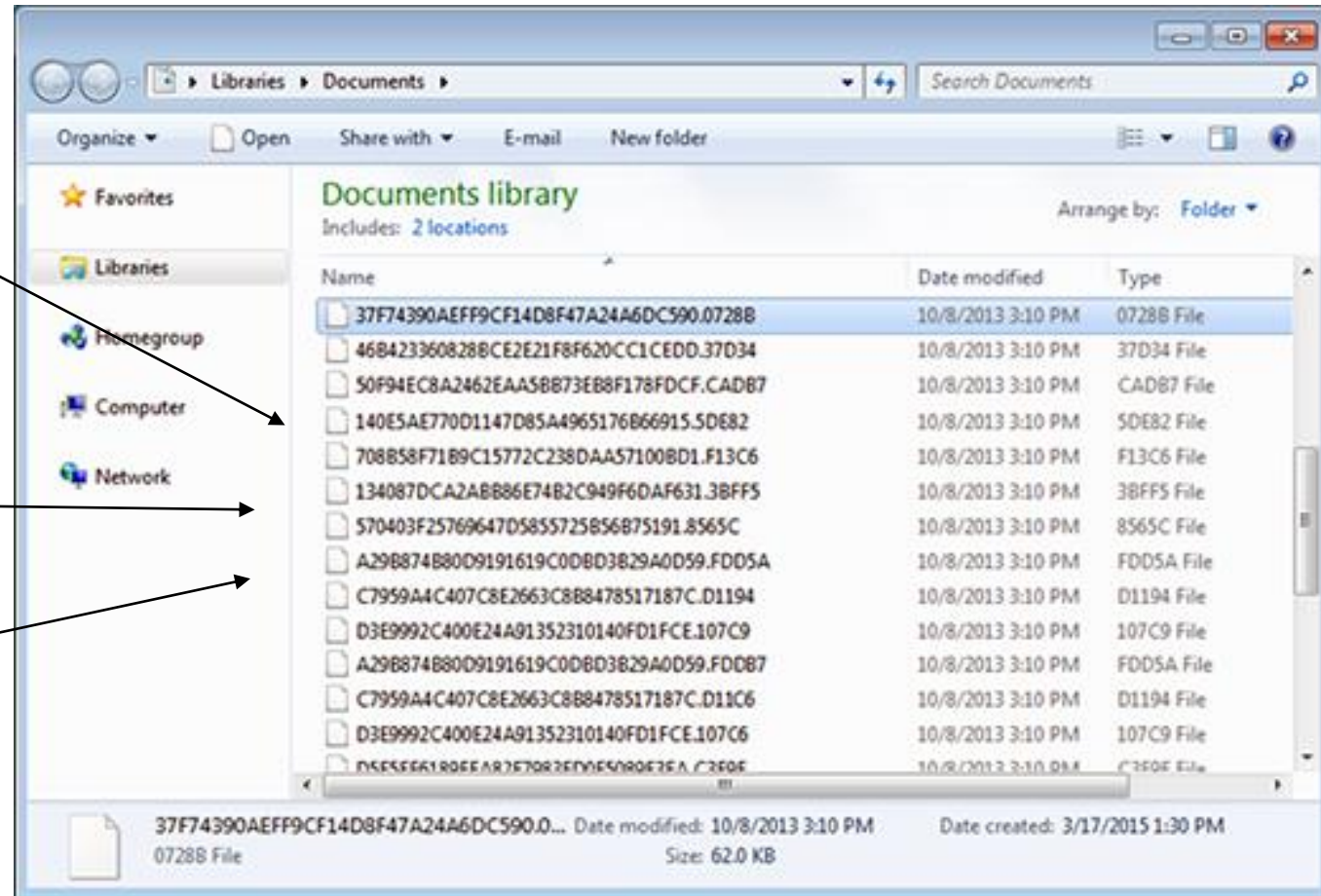
✓ קיים "שירות לקוחות"

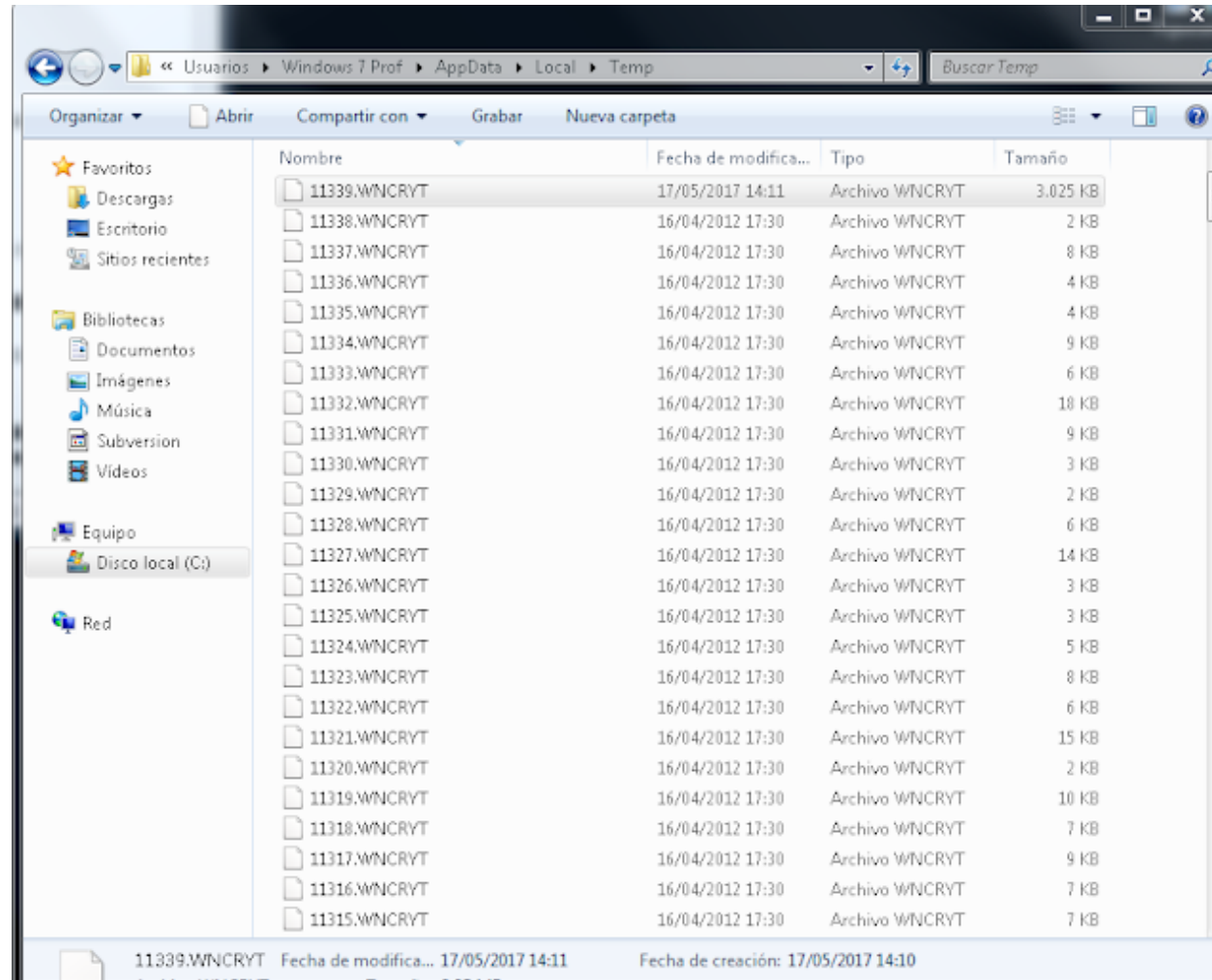
✓ הדרכה לרכישת ביטקוין

✓ המלצה להסיר אנטי-וירוס כדי שהכופרה לא תמחק

✓ אופציה להצגת המסמכים המוצפנים

לאחר הצפנת הקבצים ע"י וירוס כופרה הם נראים כך:

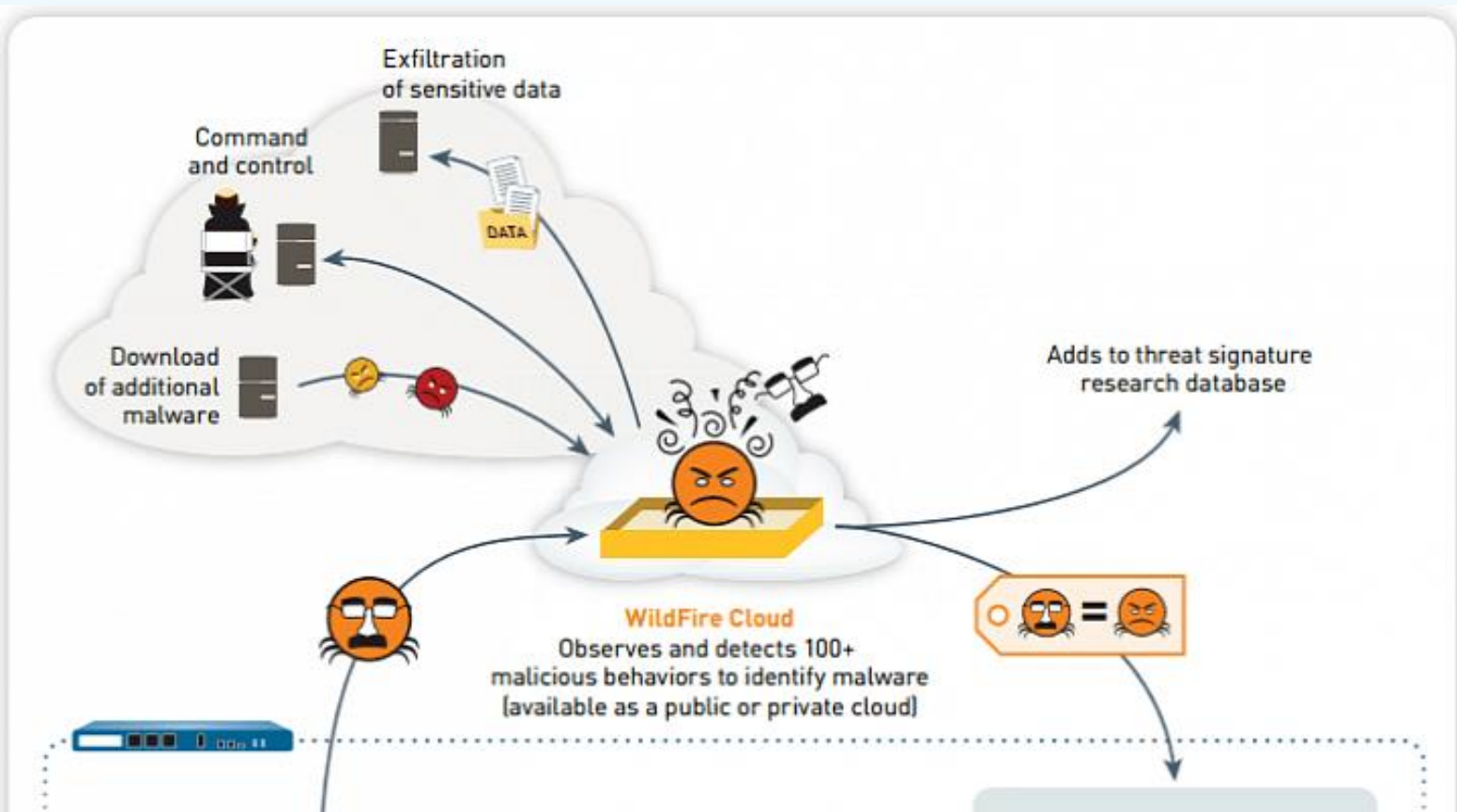




איך מגינים בפני ZERO DAY ?

SAND BOX – ארגז חול





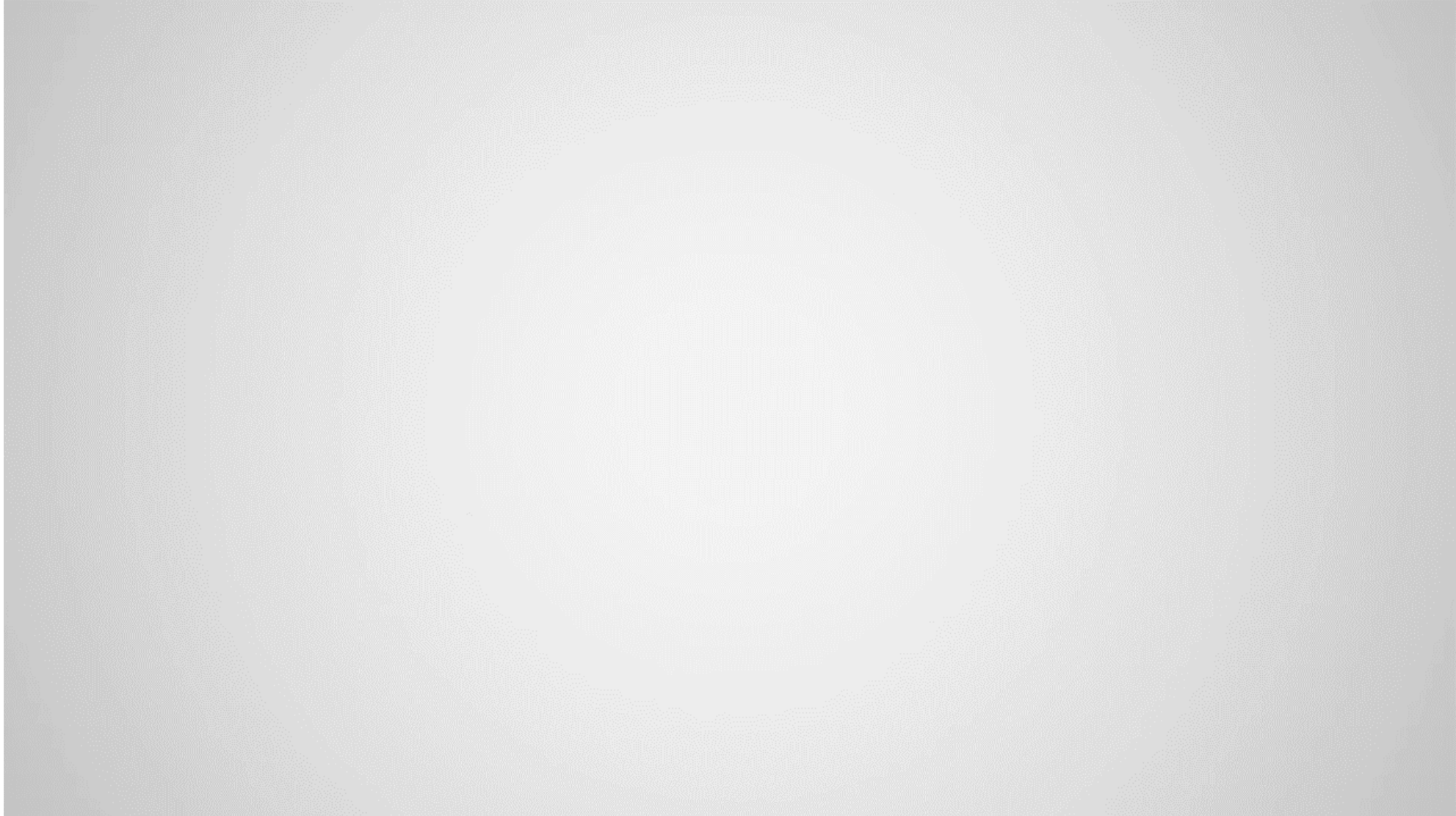
מאפיינים חשובים:

- העברת מידע מחוץ לארגון
- תקשורת עם C & C
- הורדת קבצים פנימה לארגון
- שינוי ערכים ב-REGISTRY
- נגיעה / שימוש / שינוי בקבצי מערכת
- התנהגות שלא מתאימה לקובץ המדובר

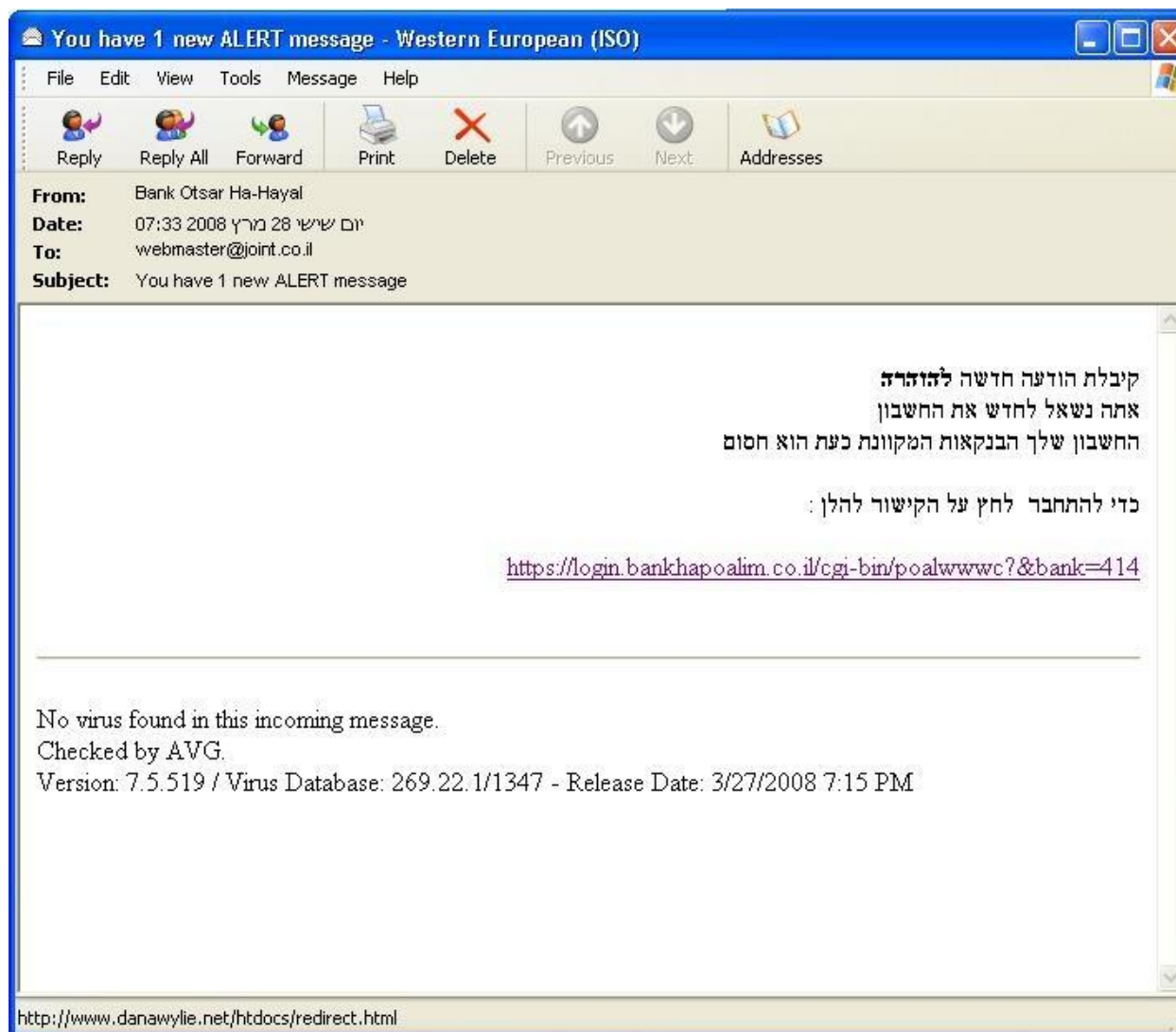
SAND BOX – ארגז חול

כיצד דפדפן כרום עושה שימוש בארגז חול – סרטון





התקפות פישינג



אתם מקבלים דוא"ל:

ואז מתקבל הדף הבא.....

תמיכה לשירותך

בנק אוצר החייל

ברוכים הבאים לאוצר באינטרנט

לצורך כניסה לשירות יש להקליד את הפרטים המזהים וללחוץ על "כניסה לחשבוןך".

קוד משתמש : ?
ת.ז. : ?
סיסמא : ?

נחסמה/ שכחת סיסמתך? [כניסה לחשבוןך](#)

אתר זה מאובטח בשיטות אבטחת המידע המתקדמות ביותר. לחצ'י כאן לפרטים נוספים.

© כל הזכויות שמורות לבנק הפועלים [תנאי גישה](#)

תמיכה לשירותך

בנק אוצר החייל

מידע למנוי חדש <

הדגמות <

הצטרפות לשירות <

הטבות באינטרנט ★

ברוכים הבאים לאוצר באינטרנט

טופס און-ליין עבור חידוש השירותים
נא לספק את המידע להלן. מילוי כל המידע חובה, פרט למקרה בו קיימים הנחיות במובן של

שם מלא :

כתובת :

יישוב :

כתובת דוא"ל :

מספר כרטיס :

תוקף הכרטיס :

מספר זהות אישי :

אתר זה מאובטח בשיטות אבטחת המידע המתקדמות ביותר.

[לחצו כאן לפרטים נוספים...](#)

© כל הזכויות שמורות לבנק הפועלים תנאי גישה

לאחר שהקורבן מזין את הפרטים גם כאן, הוא מופנה לעמוד שמוסר לו להמתין יומיים עד שהמידע יעודכן.