



# סימאות ואבטחת מידע 2023

אבי אבידן



המצב שאנו מכירים

הסיסמה הראשונה (במחשבים) נוצרה בשנת 1961

ונפרצה לאחר כשנתיים

כיום אנחנו נדרשים למס' רב של סיסמאות בשירותים

השונים אליהם אנו מנויים.

הכללים שאליהם הורגלו עד כה הופכים להיות פחות

רלוונטיים

שאלות האבטחה חוזרות על עצמן, כגון:

באיזו עיר גדלת ?

מהו שם חיית המחמד שלך ?

מה תאריך הלידה שלך ?





המצב שאנו מכירים

הסיסמה הראשונה (במחשבים) נוצרה בשנת 1961

**ונפרצה לאחר כשנתיים.**

כיום אנחנו נדרשים למס' רב של סיסמאות בשירותים

השונים אליהם אנו מנויים.

הכללים שאליהם הורגלו עד כה הופכים להיות פחות

רלוונטיים

שאלות האבטחה חוזרות על עצמן, כגון:

באיזו עיר גדלת ?

מהו שם חיית המחמד שלך ?

מה תאריך הלידה שלך ?



המצב שאנו מכירים

הסיסמה הראשונה (במחשבים) נוצרה בשנת 1961

ונפרצה לאחר כשנתיים.

**כיום אנחנו נדרשים למס' רב של סיסמאות בשירותים**

**השונים אליהם אנו מנויים.**

הכללים שאליהם הורגלו עד כה הופכים להיות פחות

רלוונטיים

שאלות האבטחה חוזרות על עצמן, כגון:

באיזו עיר גדלת ?

מהו שם חיית המחמד שלך ?

מה תאריך הלידה שלך ?



המצב שאנו מכירים

הסיסמה הראשונה (במחשבים) נוצרה בשנת 1961

ונפרצה לאחר כשנתיים.

כיום אנחנו נדרשים למס' רב של סיסמאות בשירותים

השונים אליהם אנו מנויים.

**הכללים שאליהם הורגלו עד כה הופכים להיות פחות**

**רלוונטיים.**

שאלות האבטחה חוזרות על עצמן, כגון:

באיזו עיר גדלת ?

מהו שם חיית המחמד שלך ?

מה תאריך הלידה שלך ?





המצב שאנו מכירים

הסיסמה הראשונה (במחשבים) נוצרה בשנת 1961

ונפרצה לאחר כשנתיים.

כיום אנחנו נדרשים למס' רב של סיסמאות בשירותים

השונים אליהם אנו מנויים.

הכללים שאליהם הורגלו עד כה הופכים להיות פחות

רלוונטיים

**שאלות האבטחה חוזרות על עצמן, כגון:**

**באיזו עיר גדלת ?**

**מהו שם חיית המחמד שלך ?**

**מה תאריך הלידה שלך ?**



אז איך סיסמה נפרצת ?

כיום, הדרך הפשוטה ביותר הינה ע"י שימוש בטכנית

Phishing

אפשרות נוספת שקיימת הינה Password Spraying

Online

Brute Force / Dictionary

Offline

Rainbow Table

אפשרויות נוספות:

MITM

Key Logger



אז איך סיסמה נפרצת ?

כיום, הדרך הפשוטה ביותר הינה ע"י שימוש בטכנית

Phishing

אפשרות נוספת שקיימת הינה Password Spraying

Online

Brute Force / Dictionary

Offline

Rainbow Table

אפשרויות נוספות:

MITM

Key Logger





אז איך סיסמה נפרצת ?

כיום, הדרך הפשוטה ביותר הינה ע"י שימוש בטכנית

Phishing

**אפשרות נוספת שקיימת הינה Password Spraying**

Online

Brute Force / Dictionary

Offline

Rainbow Table

אפשרויות נוספות:

MITM

Key Logger



אז איך סיסמה נפרצת ?

כיום, הדרך הפשוטה ביותר הינה ע"י שימוש בטכנית

Phishing

אפשרות נוספת שקיימת הינה Password Spraying

Online

Brute Force / Dictionary

Offline

Rainbow Table

אפשרויות נוספות:

MITM

Key Logger



אז איך סיסמה נפרצת ?

כיום, הדרך הפשוטה ביותר הינה ע"י שימוש בטכנית

Phishing

אפשרות נוספת שקיימת הינה Password Spraying

Online

Brute Force / Dictionary

Offline

Rainbow Table

אפשרויות נוספות:

MITM

Key Logger





אז איך סיסמה נפרצת ?

כיום, הדרך הפשוטה ביותר הינה ע"י שימוש בטכנית

Phishing

אפשרות נוספת שקיימת הינה Password Spraying

Online

Brute Force / Dictionary

Offline

Rainbow Table

**אפשרויות נוספות:**

MITM

Key Logger



אז מהן ההמלצות לסיסמא ב-2023 ?

**העדיפו סיסמא ארוכה ע"פ סיסמא מורכבת**

המנעו מאיפוס סיסמא תדירים

אפשרו למשתמשים לבצע העתקת סיסמא

חסמו את האפשרות לסיסמא מוכרת

חסמו את האפשרות לחזרה על סיסמאות

הגבילו את מס' ניסיונות הגישה האפשריים

בצעו שימוש ככל הניתן ב- 2FA / MFA

הטמיעו \ אפשרו מנגנון Salting בעת שמירת סיסמאות



אז מהן ההמלצות לסיסמא ב-2023 ?

העדיפו סיסמא ארוכה ע"פ סיסמא מורכבת

**המנעו מאיפוס סיסמא תדירים**

אפשרו למשתמשים לבצע העתקת סיסמא

חסמו את האפשרות לסיסמא מוכרת

חסמו את האפשרות לחזרה על סיסמאות

הגבילו את מס' ניסיונות הגישה האפשריים

בצעו שימוש ככל הניתן ב- 2FA / MFA

הטמיעו \ אפשרו מנגנון Salting בעת שמירת סיסמאות





אז מהן ההמלצות לסיסמא ב-2023 ?

העדיפו סיסמא ארוכה ע"פ סיסמא מורכבת

המנעו מאיפוס סיסמא תדירים

**אפשרו למשתמשים לבצע העתקת סיסמא**

חסמו את האפשרות לסיסמא מוכרת

חסמו את האפשרות לחזרה על סיסמאות

הגבילו את מס' ניסיונות הגישה האפשריים

בצעו שימוש ככל הניתן ב- 2FA / MFA

הטמיעו \ אפשרו מנגנון Salting בעת שמירת סיסמאות



אז מהן ההמלצות לסיסמא ב-2023 ?

העדיפו סיסמא ארוכה ע"פ סיסמא מורכבת

המנעו מאיפוס סיסמא תדירים

אפשרו למשתמשים לבצע העתקת סיסמא

**חסמו את האפשרות לסיסמא מוכרת**

חסמו את האפשרות לחזרה על סיסמאות

הגבילו את מס' ניסיונות הגישה האפשריים

בצעו שימוש ככל הניתן ב- 2FA / MFA

הטמיעו \ אפשרו מנגנון Salting בעת שמירת סיסמאות



אז מהן ההמלצות לסיסמא ב-2023 ?

העדיפו סיסמא ארוכה ע"פ סיסמא מורכבת

המנעו מאיפוס סיסמא תדירים

אפשרו למשתמשים לבצע העתקת סיסמא

חסמו את האפשרות לסיסמא מוכרת

**חסמו את האפשרות לחזרה על סיסמאות**

הגבילו את מס' ניסיונות הגישה האפשריים

בצעו שימוש ככל הניתן ב- 2FA / MFA

הטמיעו \ אפשרו מנגנון Salting בעת שמירת סיסמאות





אז מהן ההמלצות לסיסמא ב-2023 ?

העדיפו סיסמא ארוכה ע"פ סיסמא מורכבת

המנעו מאיפוס סיסמא תדירים

אפשרו למשתמשים לבצע העתקת סיסמא

חסמו את האפשרות לסיסמא מוכרת

חסמו את האפשרות לחזרה על סיסמאות

**הגבילו את מס' ניסיונות הגישה האפשריים**

בצעו שימוש ככל הניתן ב- 2FA / MFA

הטמיעו \ אפשרו מנגנון Salting בעת שמירת סיסמאות



אז מהן ההמלצות לסיסמא ב-2023 ?

העדיפו סיסמא ארוכה ע"פ סיסמא מורכבת

המנעו מאיפוס סיסמא תדירים

אפשרו למשתמשים לבצע העתקת סיסמא

חסמו את האפשרות לסיסמא מוכרת

חסמו את האפשרות לחזרה על סיסמאות

הגבילו את מס' ניסיונות הגישה האפשריים

**בצעו שימוש ככל הניתן ב- 2FA / MFA**

הטמיעו \ אפשרו מנגנון Salting בעת שמירת סיסמאות



אז מהן ההמלצות לסיסמא ב-2023 ?

העדיפו סיסמא ארוכה ע"פ סיסמא מורכבת

המנעו מאיפוס סיסמא תדירים

אפשרו למשתמשים לבצע העתקת סיסמא

חסמו את האפשרות לסיסמא מוכרת

חסמו את האפשרות לחזרה על סיסמאות

הגבילו את מס' ניסיונות הגישה האפשריים

בצעו שימוש ככל הניתן ב- 2FA / MFA

**הטמיעו \ אפשרו מנגנון Salting בעת שמירת סיסמאות**



מדיניות ואכיפה

קיבוע מדיניות סיסמאות

תיעוד – ע"י איסוף ושמירת לוגים.

הפצה

תרגול ומודעות

**Password vs passphrase**

PASSWORD	PASSPHRASE
USERNAME .....	USERNAME .....
PASSCODE Pa\$\$w0rd!	PASSCODE Tally onyx lulu bee
DIFFICULTY TO REMEMBER Hard	DIFFICULTY TO REMEMBER Easy
DIFFICULTY TO HACK Easy	DIFFICULTY TO HACK Hard
COMMON CHARACTERISTICS Base word, capitalization, character substitutions, punctuation and numbers	COMMON CHARACTERISTICS Random common words, up to 100 characters in length

מדיניות ואכיפה

קיבוע מדיניות סיסמאות

תיעוד – ע"י איסוף ושמירת לוגים.

הפצה

תרגול ומודעות

**Password vs passphrase**

PASSWORD	PASSPHRASE
USERNAME .....	USERNAME .....
PASSCODE Pa\$\$w0rd!	PASSCODE Tally onyx lulu bee
DIFFICULTY TO REMEMBER Hard	DIFFICULTY TO REMEMBER Easy
DIFFICULTY TO HACK Easy	DIFFICULTY TO HACK Hard
COMMON CHARACTERISTICS Base word, capitalization, character substitutions, punctuation and numbers	COMMON CHARACTERISTICS Random common words, up to 100 characters in length

מדיניות ואכיפה

קיבוע מדיניות סיסמאות

תיעוד – ע"י איסוף ושמירת לוגים.

הפצה

תרגול ומודעות





מדיניות ואכיפה

קיבוע מדיניות סיסמאות

תיעוד – ע"י איסוף ושמירת לוגים.

הפצה

תרגול ומודעות





כלים ופתרונות

אפשרות שימוש ב-MFA

Something you Know

Something you have

Something you are

הקצו רק הרשאות אשר חובה לביצוע המשימה ולא יותר

אכפו מדיניות סיסמאות ושמירת לוגים

הגבילו את מספר ניסיונות הגישה

עשו שימוש ב-SSO באמצעות שירותים כגון Microsoft Azure, OKTA

אפשרו שימוש במנהלי סיסמאות כולל יכולת העתקה



כלים ופתרונות

אפשרות שימוש ב-MFA

Something you Know

Something you have

Something you are

**הקצו רק הרשאות אשר חובה לביצוע המשימה ולא יותר**

אכפו מדיניות סיסמאות ושמירת לוגים

הגבילו את מספר ניסיונות הגישה

עשו שימוש ב-SSO באמצעות שירותים כגון Microsoft Azure, OKTA

אפשרו שימוש במנהלי סיסמאות כולל יכולת העתקה





כלים ופתרונות

אפשרות שימוש ב-MFA

Something you Know

Something you have

Something you are

הקצו רק הרשאות אשר חובה לביצוע המשימה ולא יותר

**אכפו מדיניות סיסמאות ושמירת לוגים**

הגבילו את מספר ניסיונות הגישה

עשו שימוש ב-SSO באמצעות שירותים כגון Microsoft Azure, OKTA

אפשרו שימוש במנהלי סיסמאות כולל יכולת העתקה



כלים ופתרונות

אפשרות שימוש ב-MFA

Something you Know

Something you have

Something you are

הקצו רק הרשאות אשר חובה לביצוע המשימה ולא יותר

אכפו מדיניות סיסמאות ושמירת לוגים

**הגבילו את מספר ניסיונות הגישה**

עשו שימוש ב-SSO באמצעות שירותים כגון Microsoft Azure, OKTA

אפשרו שימוש במנהלי סיסמאות כולל יכולת העתקה



כלים ופתרונות

אפשרות שימוש ב-MFA

Something you Know

Something you have

Something you are

הקצו רק הרשאות אשר חובה לביצוע המשימה ולא יותר

אכפו מדיניות סיסמאות ושמירת לוגים

הגבילו את מספר ניסיונות הגישה

עשו שימוש ב-SSO באמצעות שירותים כגון Microsoft Azure, OKTA

אפשרו שימוש במנהלי סיסמאות כולל יכולת העתקה





כלים ופתרונות

אפשרות שימוש ב-MFA

Something you Know

Something you have

Something you are

הקצו רק הרשאות אשר חובה לביצוע המשימה ולא יותר

אכפו מדיניות סיסמאות ושמירת לוגים

הגבילו את מספר ניסיונות הגישה

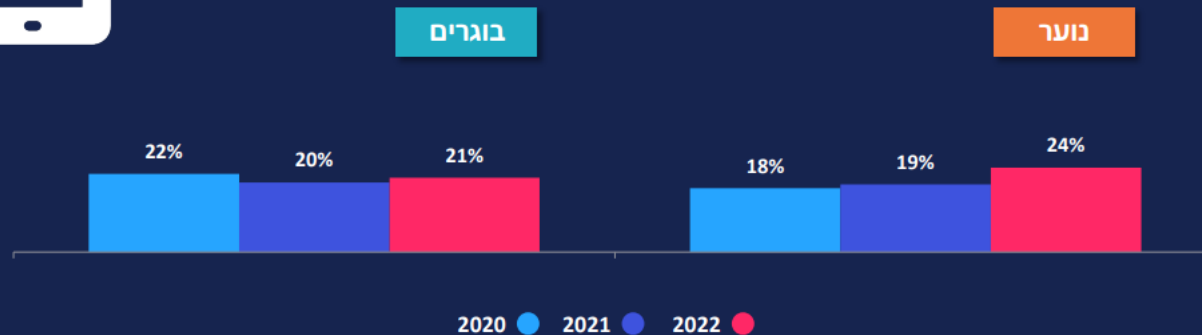
עשו שימוש ב-SSO באמצעות שירותים כגון Microsoft Azure, OKTA

**אפשרו שימוש במנהלי סיסמאות כולל יכולת העתקה**

Password-based attacks are the primary method by which accounts are compromised.

## חוו פריצה למייל או לחשבון ברשת ח

% שחוו פריצה



### Deezer

In late 2022, the music streaming service Deezer disclosed a data breach. The breach dated back to a mid-2019 backup exposed by a 3rd party and then broadly redistributed on a popular hacking forum. Impacted data included IP addresses, names, usernames, genders, DoBs and the geographical locations of users.

**Breach date:** 22 April 2019

**Date added to HIBP:** 2 January 2023

**Compromised accounts:** 229,037,936

**Compromised data:** Dates of birth, Email addresses, Genders, Geographical locations

**Compromised data:** Spoken languages, Usernames

## Some useful links:

1. <https://haveibeenpwned.com/>
2. [https://www.gov.il/he/departments/israel\\_national\\_cyber\\_directorate/govil-landing-page](https://www.gov.il/he/departments/israel_national_cyber_directorate/govil-landing-page)
3. <https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide>
4. Cyber.gov.il
5. <https://www.gov.il/he/departments/general/topten>



Q & A ? !



