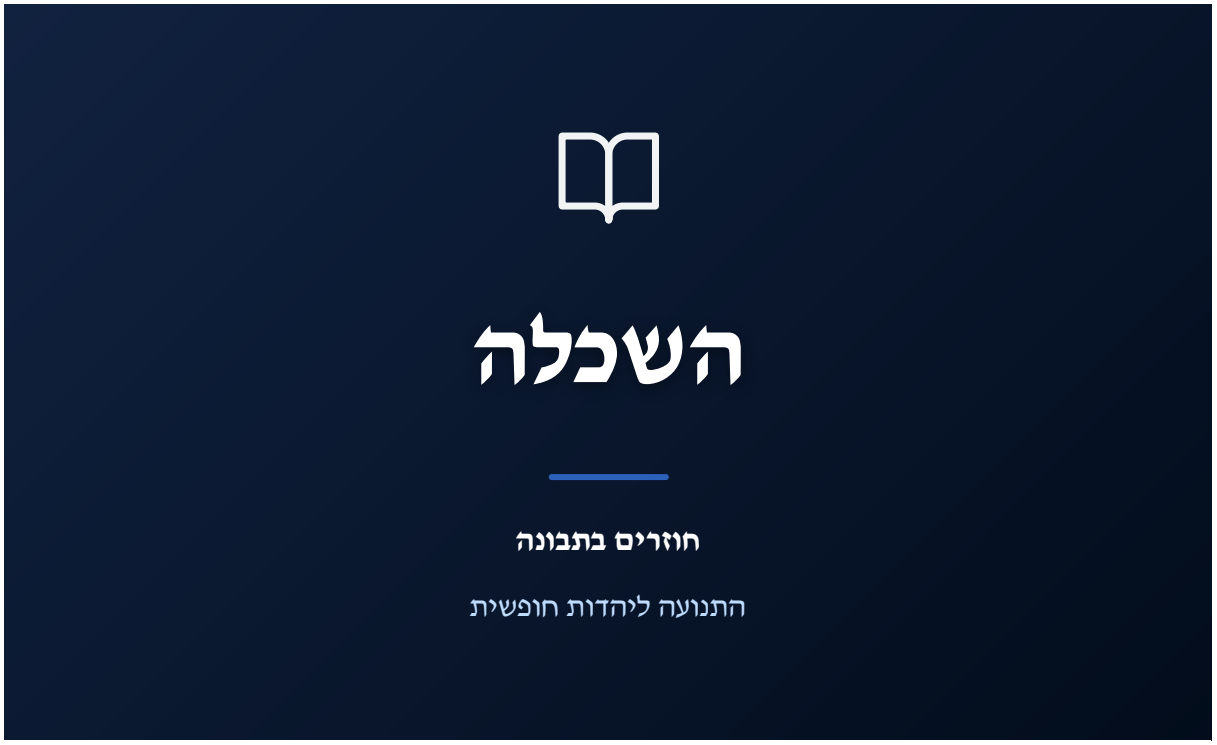


# אבטחת מידע בסיסית

פרויקט השכלה : גישה חופשית לידע ולמיומנויות חיים

# תוכן עניינים

**אבטחת מידע בסיסית** הוא ספר לימוד המיועד להקניית ידע בסיסי בתחום אבטחת מידע וסייבר. הספר מכסה נושאים כמו הגנה על מחשב אישי, סיסמאות, גלישה בטוחה, והתמודדות עם איומים.

# מבוא והגורם האנושי

## מבוא והגורם האנושי

### מהי אבטחת מידע?

אבטחת מידע היא הגנה על מידע מפני גישה, שימוש, חשיפה, שינוי או השמדה בלתי מורשים.

### שלושת עמודי אבטחת המידע (CIA)

- **סודיות** (Confidentiality) — רק מורשים יגשו למידע
- **שלמות** (Integrity) — המידע לא שונה ללא הרשאה
- **זמינות** (Availability) — המידע נגיש כשצריך

### הגורם האנושי

**הגורם האנושי** הוא החוליה החלשה ביותר באבטחת מידע. רוב הפריצות מתחילות בטעות אנושית: לחיצה על קישור זדוני, שיתוף סיסמה, הורדת קובץ נגוע.

### הנדסה חברתית (Social Engineering)

מניפולציה פסיכולוגית שמטרתה לגרום לאדם לחשוף מידע או לבצע פעולה.

# הגנה על המחשב האישי

## הגנה על המחשב האישי

### עדכוני תוכנה

עדכנו תמיד את מערכת ההפעלה והתוכנות. עדכונים סוגרים פרצות אבטחה.

### תוכנת אנטי-וירוס

התקינו תוכנת אנטי-וירוס ועדכנו אותה באופן שוטף.

### חומת אש (Firewall)

חומת אש מסננת תעבורת רשת ומונעת גישה בלתי מורשית.

### גיבוי

גבו את הנתונים שלכם באופן קבוע — על דיסק חיצוני או בענן.

### תוכנות מומלצות

- אנטי-וירוס: Windows Defender (מובנה), או תוכנות חינמיות כמו Avast, AVG
- חומת אש: Windows Firewall (מובנה)
- גיבוי: כלי הגיבוי המובנה או שירותי ענן

# סיסמאות ואיך לשמור עליהן

## סיסמאות ואיך לשמור עליהן

### סיסמה חזקה

- אורך: לפחות 12 תווים
- שילוב: אותיות גדולות וקטנות, מספרים, סימנים מיוחדים
- ייחודית: סיסמה שונה לכל שירות
- לא ניתנת לניחוש: לא שם, תאריך לידה, או מילה מהמילון

### מנהל סיסמאות

מנהל סיסמאות (Password Manager) הוא תוכנה שמאחסנת את כל הסיסמאות שלכם בצורה מוצפנת.

### אימות דו-שלבי (2FA)

הפעילו אימות דו-שלבי בכל מקום אפשרי — שכבת הגנה נוספת.

### מה לא לעשות

- לא לשתף סיסמאות
- לא לכתוב על פתק
- לא להשתמש באותה סיסמה בכל מקום
- לא להתחבר ממחשבים ציבוריים

# תקשורת מאובטחת ורשתות אלחוטיות

## תקשורת מאובטחת, רשתות אלחוטיות וגלישה אנונימית

### HTTPS

גלשו רק באתרים עם HTTPS (מנעול בשורת הכתובת). HTTPS מצפין את התקשורת.

### רשתות Wi-Fi

- הצפינו את הרשת הביתית (WPA2/WPA3)
- שנו את סיסמת ברירת המחדל של הנתב
- היזהרו מרשתות Wi-Fi ציבוריות — הימנעו מפעולות רגישות

### VPN

VPN (Virtual Private Network) מצפין את כל התעבורת שלכם ומסתיר את כתובת ה-IP.

### גלישה אנונימית

- מצב גלישה פרטית בדפדפן
- דפדפן Tor לאנונימיות מתקדמת

### דוא״ל מאובטח

השתמשו בשירותי דוא״ל מאובטחים והיזהרו מצרופות וקישורים חשודים.

# איומים נפוצים פישינג והאקרים

## איומים נפוצים: פישינג והאקרים

### פישינג (Phishing)

ניסיון להונות באמצעות הודעות מזויפות (דוא"ל, SMS) שנראות כאילו הגיעו ממקור אמין.

**איך מזהים פישינג?**

- כתובת שולח חשודה
- טעויות כתיב
- בקשה דחופה לפעולה
- קישורים מוזרים
- בקשה למסור פרטים אישיים

### האקרים

האקרים הם אנשים שמנצלים חולשות במערכות מחשב. סוגים: תוכנות כופר (Ransomware), וירוסים, תולעים, סוסים טרויאניים.

### כיצד להתגונן?

- לא ללחוץ על קישורים חשודים
- לבדוק כתובות URL
- לא להוריד קבצים ממקורות לא מוכרים
- לעדכן תוכנות
- להפעיל אימות דו-שלבי

# הגנה על טלפונים ניידים וביומטריה

## הגנה על טלפונים ניידים, מצלמות, זיהוי ביומטרי ותגי רדיו

### הגנה על הטלפון

- נעילת מסך (סיסמה, דפוס, טביעת אצבע)
- עדכון מערכת ההפעלה
- הורדת אפליקציות רק מחנויות רשמיות
- גיבוי תמונות ואנשי קשר
- הצפנת המכשיר

### זיהוי ביומטרי

זיהוי על בסיס מאפיינים פיזיים:

- **טביעת אצבע** — נפוצה בטלפונים
- **זיהוי פנים** — Face ID
- **סריקת קשתית** — ברמת אבטחה גבוהה

### מצלמות

כסו את מצלמת המחשב הנייד כשאינכם משתמשים בה. היזהרו מאפליקציות שמבקשות גישה למצלמה.

### תגי רדיו (RFID)

RFID משמש בכרטיסי עובד, כרטיסי אשראי ללא מגע ותגי זיהוי. סכנות: קריאה מרחוק ללא ידיעת הבעלים.

**הופק ע״י חוזרים בתבונה · betvuna.com**

מקור התוכן : ויקיספר — רישיון CC BY-SA 4.0 · התוכן עובד והותאם