מצגת היערכות לשבוע הגלישה הבטוחה ברשת תשע״ח

הקו המנחה של תכנית "חיים ברשת" המופעלת ע"י אגף טכנולוגיות מידע בשנת תשע"ח מתמקד בגלישה נבונה ואחראית ברשת כשיגרה בשני צירים:

ישראל וברחבי העולם ישנה מגמה של עלייה בשילוב טכנולוגיות מידע בחינוך. מגמה זו מביאה עימה עלייה בסיכוני הסייבר ואבטחת המידע. מתקפות סייבר עלולות לפגוע בארגונים וביחידים, להביא לעצירת תהליכים עסקיים, לפגיעה במוניטין ולדליפה של מידע רגיש.

במשרד החינוך רואים חשיבות

רבה בנקיטת מרב האמצעים להגנה על תלמידים מפני איומי סייבר ולחינוך להרגלים נכונים בסביבות טכנולוגיות

פעילות החינוך, ההסברה והמניעה בנושא זה מהווה את אחד המרכיבים המרכזיים
במאמץ של המשרד לקידום התנהלות מיטבית במרחב הסייבר
בדגש על תלמידים, מורים והורים במערכת החינוך
והיא מתמקדת בשלושה היבטים מרכזיים:

סודיות המידע

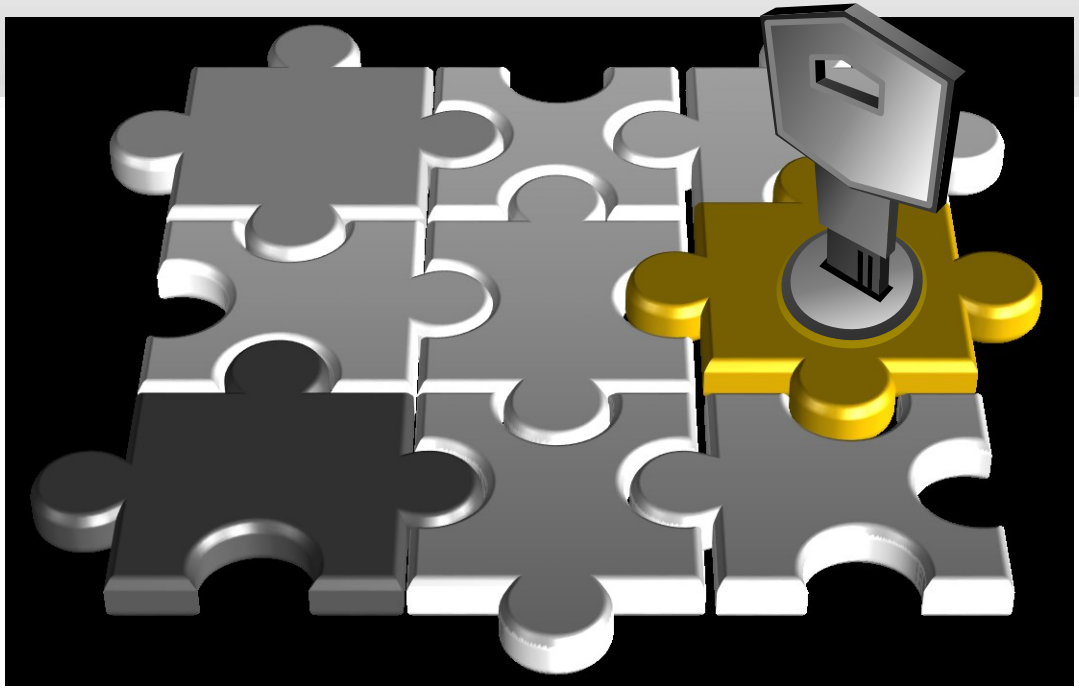
הגבלת גישה למידע ושמירה על פרטיות.

שלמות מידע

הגנה מפני שינוי זדוני של המידע.

זמינות מידע

שמירה על זמינות ויעילות הגישה אל המידע.



סיכוני סייבר במגזר החינוך

"רמאות פדגוגית"

השחתת אתרים

אירועי טוזקה

פגיעה בפרטיות

תכנים לא הולמים

פשיעה ובריונות

פגיעה בחירום

השבתת שירותים

הנחיות לגבי המדיניות

לשם כך המשרד מפרסם הנחיות מפורטות לגבי המדיניות בנושא אבטחת מידע והגנה בסייבר
מסמך ההנחיות לאבטחת מידע למוסדות חינוך
והמוגדרת גם בחוזר מנכ"ל:

1. חוזר מנכ"ל - אתיקה ומוגנות ברשת
2. חוזר מנכ"ל - שמירה על פרטיות באתרי האינטרנט
3. חוזר מנכ"ל - חסימת אתרים בלתי רצויים
4. חוזר מנכ"ל - שימוש מושכל בטלפונים סלולריים -
5. חוזר מנכ"ל - שילוב ציוד תקשורת והתקני קצה בבתי הספר

בנושא השמירה על מידע רגיש בבתי הספר המשרד מדריך את העובדים בנושאים אלו על מנת למנוע מצבים שעלולים לגרום להם למסור מידע רגיש באמצעות הטעיה והונאות

בנושא השימוש בספקי תוכן ובשירותי ענן בבית הספר המשרד מפרסם בענן החינוכי קטלוג של אפליקציות וספקי תוכן מאושרים לשימוש על ידי בתי הספר.

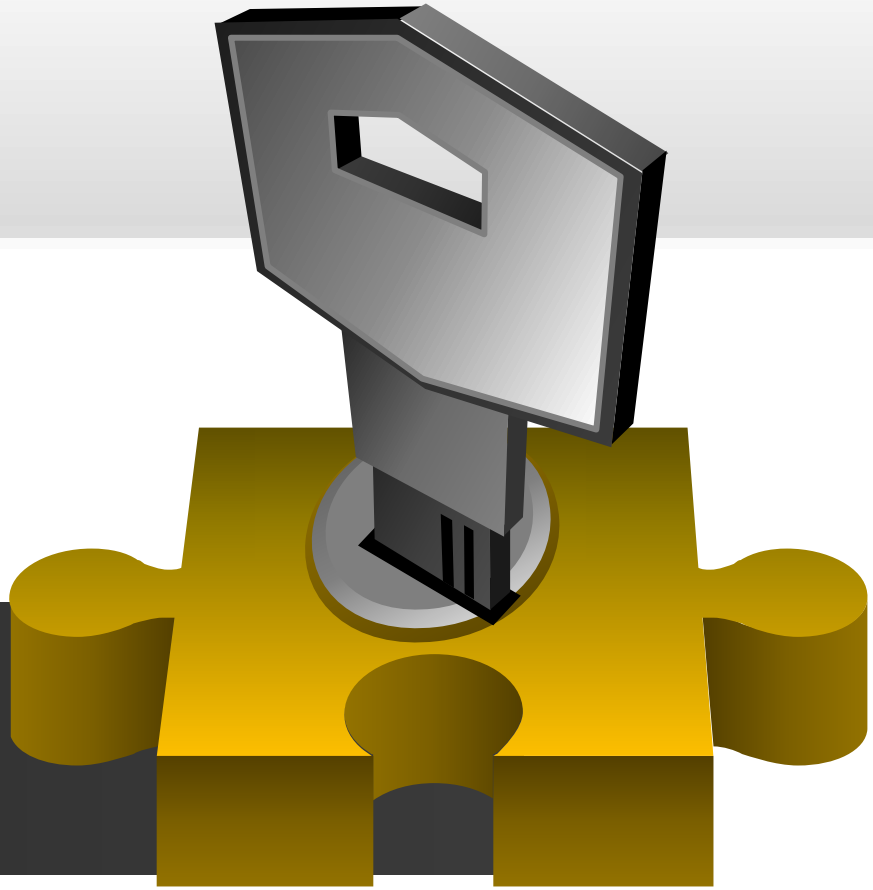
שמירת הפרטיות באתרי האינטרנט הבית ספריים".

אתרי אינטרנט אתר בית ספרי יוקם בהתאם להנחיות בחוזר מנכ"ל: "שמירת הפרטיות באתרי האינטרנט הבית ספריים".
סינון אתרים ותוכן לא ראוי יש לוודא כי הגישה מבית הספר לרשת האינטרנט נעשית תמיד באמצעות מנגנוני סינון לחסימת תכנים שאינם ראויים ונוזקות, כפי שמפורט בחוזר מנכ"ל – **שמירה על הפרטיות באתרי האינטרט הבית-ספריים**

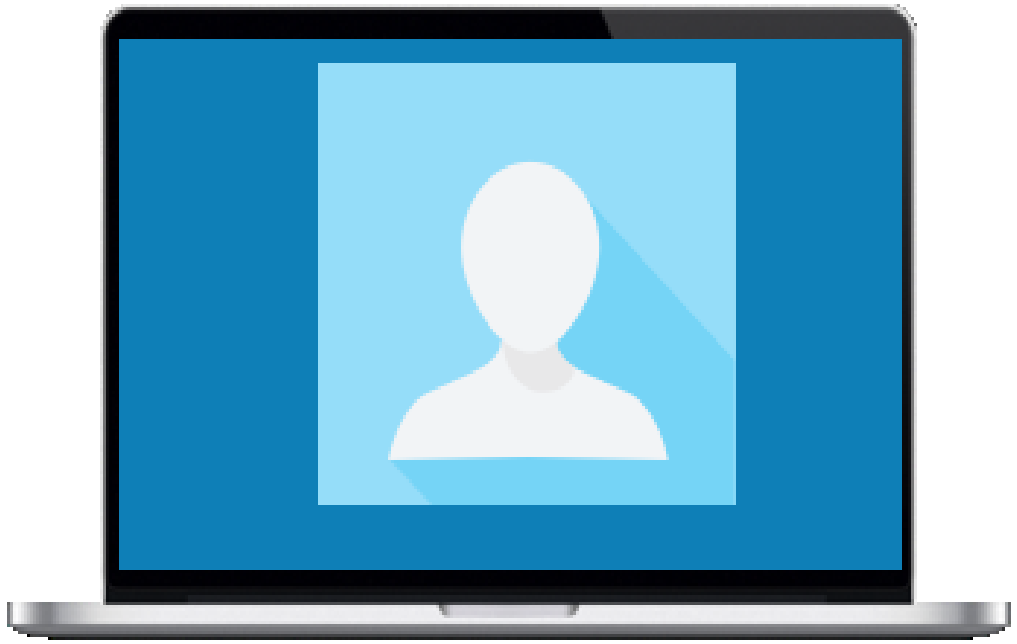
שימו לב!

יש לדווח על כל אירוע אבטחת מידע בבית הספר ליחידת ההגנה בסייבר למגזר החינוך zivko@education.gov.il!

סיכוני סייבר במערכת החינוך – מה יכול להדאיג אותי?



- ✓ גישת תלמידים למידע שלא אמורים להיחשף אליו.
- ✓ שמירה על פרטיות התלמידים.
- ✓ שמירה על הפרטיות שלי בעת גלישה ברשת.



- ✓ הגנה על המידע שלי במידה ומכשיר נגנב/ אובד.
- ✓ הגנה על מכשירים ניידים (טלפונים, טאבלטים).
- ✓ הגנה על עצמנו מהונאות, גניבת זהות

- ✓ הידבקות בווירוסים, ונוזקות ותוכנות מזיקות אחרות.
- ✓ חוסר בידע, התמודדות עם אירוע אבטחה

כלים להתמודדות – שמירה על פרטיות, לתלמידים

שימוש בהזדהות חזקה.

נעילת מחשב עם סיסמא בכל פעם שעוזבים אותו

יציאה (log out) מאפליקציות שונות

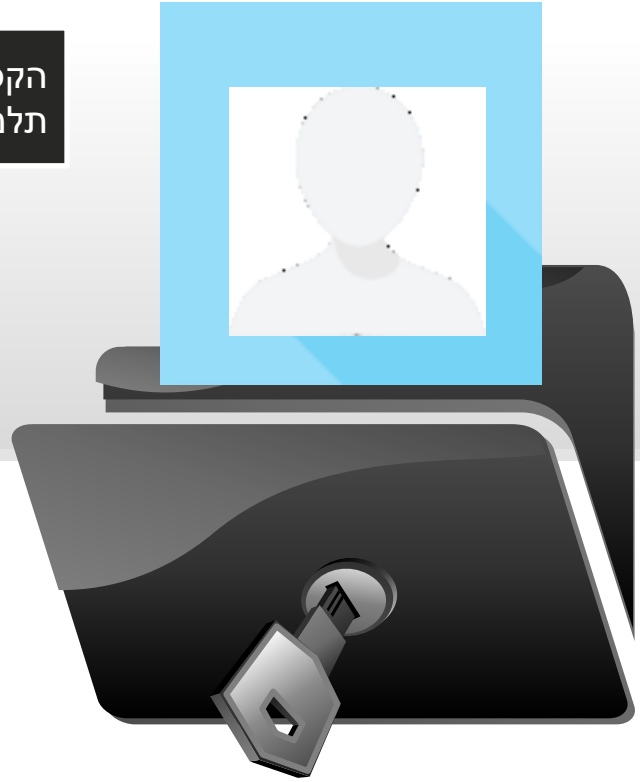
ללמד כיצד לזהות אימיילים מתחזים

על מנת לזכור את כל הסיסמאות: עשו שימוש במנהל סיסמאות

בחרו סיסמאות שונות וחזקות לשירותים וחשבונות שונים

כלים להתמודדות – שמירה על פרטיות תלמידים, לצוות החינוכי.

1. הקפידו על האופן בו אתם שומרים מידע פרטי (רשימות תלמידים, תמונות, ציונים, אבחונים אישיותיים)
2. העברת מידע מוגן – **לא** באמצעות חשבון האימייל הפרטי
3. שמירת מידע מוגן - במערכות יעודיות כגון מנב"ס, משוב וכד'. לא לשמור קבצים ב Google drive הפרטי
4. למדו את התלמידים לבצע יציאה (log out) מהחשבונות השונים על מחשבי בית הספר – gmail, Facebook, אפליקציות חינוכיות ועוד.
5. עודדו את הילדים **לא לשמור** סיסמאות במנהל הסיסמאות של הדפדפן

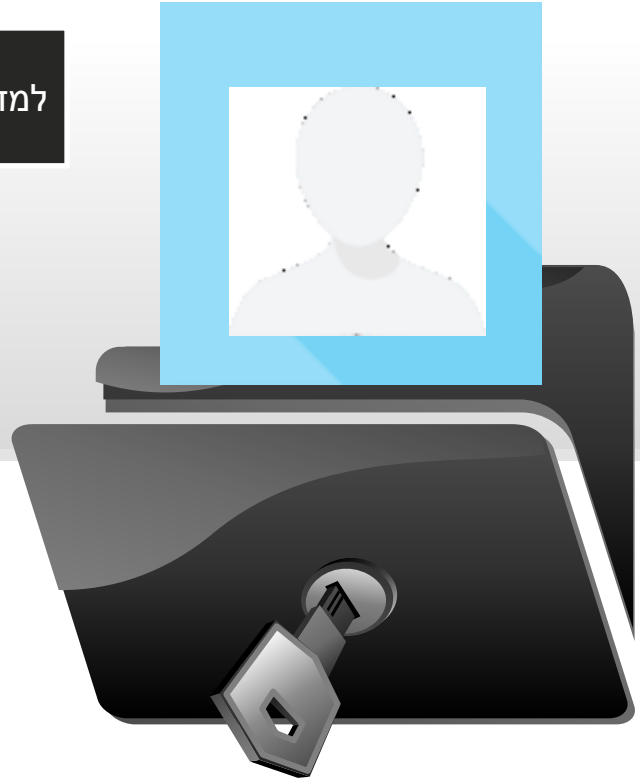


כלים להתמודדות – שמירה על פרטיות תלמידים, לצוות החינוכי.

6 למדו את התלמידים כיצד לזהות אימיילים מתחזים

7 התקינו חוסם סיסמאות על הדפדפן בו נעשה שימוש

8 למדו את הילדים כיצד לנהל את הסמאות שלהם – למשל לא לשתף את הסמאות עם חברים.



כלים להתמודדות – הידבקות בוירוסים

1. ודאו כי על המחשב מותקנת תוכנת אנטי וירוס. על התוכנה להתעדכן באופן שוטף ולבצע סריקה של כלל המחשב אחת לתקופה
2. הימנעו משימוש דיסק און קי
3. התקינו עדכוני אבטחה במערכת ההפעלה – מומלץ מאוד לאפשר את Windows update על המחשב כך שהעדכונים יותקנו באופן קבוע.
4. הימנעו מהורדת קבצים המצורפים לאימיילים חשודים ומהתקנת תוכנות שאינן מאושרות לשימוש.
5. הימנעו מגלישה באתרי אינטרנט לא בטוחים (למשל כאלה שקישור אליהם התקבל באימייל ממקור לא ידוע).

כלים להתמודדות – הגנה על מידע במקרה של גניבה/אובדן

1

גיבוי מידע שבמכשירים השונים באופן קבוע

2

הצפנה של הכונן הקשיח במחשב על ידי שימוש ב המובנה ב **Bitlocker** או שימוש **Windows** במוצר הצפנה אחר

3

הצפנה של הטלפון הנייד ושל הטבלט, הפעילו את האפשרות למעקב ומחיקה מרחוק של הטלפון במידה ונגנב או אובד. (כגון find my iphone)

4

הנחיות להצפנת אנדרואיד: https://www.networkworld.com/article/3268496/how-to-encrypt-your-android-phone-and-tablet.html

5

הצפנה של הטלפון הנייד ושל הטבלט: הנחיות להצפנת iOS https://ssd.eff.org/en/module/how-encrypt-your-iphone

4

הורדת אפליקציות למכשיר הנייד – אך ורק מהחנויות הרשמיות: Google Play ו App Store.

סרטון לאיך להצפין טלפונים: https://www.cnet.com/how-to/how-to-encrypt-your-ios-or-android-device/

כלים להתמודדות – גלישה בטוחה

1

עשו שימוש בחוסם פרסומות – רבים לא יודעים זאת, אולם פרסומות רבות המופיעות באתרי אינטרנט מכילות קוד העושה שימוש במידע הקיים בדפדפן ובמחשב שלכם. התקנה של חוסם סיסמאות משפרת משמעותית את היכולת לעקוב אחריכם

2

Your text here במידה וקיבלתם אימייל המכיל קישור לאתר אינטרנט לצורך ביצוע פעולה – אל תלחצו על הקישור. במקום זאת גילשו אל האתר באופן עצמאי על מנת לוודא שלא מדובר בניסיון הונאה

3

בידקו את הגדרות אבטחת המידע והפרטיות בחשבונות ואפליקציות בהם אתם עושים שימוש:
https://securityplanner.org/#/tool/privacy-settings
https://securityplanner.org/#/tool/security-checkups

במקרה חירום יש להיעזר במומחים

מנהל יחידת אבטחת מידע בבתי ספר:
זיו קורן
zivko@education.gov.il

הרשות הלאומית להגנה בסייבר הקימה מוקד לטיפול באירועי סייבר אשר נותן מענה לאזרחים בודדים ולארגונים.
פנו ל –

.
https://www.gov.il/he/Departments/Topics/coping_with_cyber_events

9344*

קרינה

ר המדיה הדיגיטלית אשר סובבים אותנו משפרים את איכות חיינו ומאפשרים לנו
ת מיתרונות הטכנולוגיה מחד גיסא, אך מאידך גיסא הם מהווים מקור להשלכות על
בריאות האדם, בייחוד בגיל הצעיר. משרד החינוך מקפיד על יישום עקרון הזהירות המונעת
במוסדות החינוך, תוך איזון בין שימוש התלמידים באמצעי קצה ומכשירים סלולריים, לבין
ההשלכות הבריאותיות, החברתיות והכלכליות.

עיקרון הזהירות המונעת

בתחום הקרינה הבלתי מיינת, מעוגן בחקיקה בישראל. הגדרת עיקרון הזהירות בחקיקה הישראלית מופיעה בדברי ההסבר (קובץ PDF להורדה)

פעילויות לתלמידים

אוגדן פעילויות מתוך הקטלוג החינוכי בנושא אבטחת מידע

נורמות התנהגות ברשת

אבטחת מידע אישי ושמירה על הפרטיות

זכויות יוצרים

שימוש במכשירים פולטי קרינה

אז מהי בעצם ארגונומיה?

ארגונומיה זה מדע העוסק בהתאמת הסביבה למשתמש. במקרה שלנו הכוונה להתאמת עמדת המחשב החביבה עליכם כל כך למרב הנוחות שלכם ולמזעור אי נוחות וכאבים

למה בעצם כל כך חשוב לשמור על סידור וכללי עבודה ארגונומיים בעמדת המחשב?

יותר ויותר מחקרים מצביעים על עליה במספר הילדים ובני הנוער הסובלים: מצוואר תפוס, כאב בכתף ובכף היד וכאבי גב תחתון.
העבודה במחשב עלולה לגרום לתופעות שנקראות RSI – פציעות הנגרמות משימוש ממושך בג'ויסטיק, בהקלדה ממושכת בצ'אט ומישיבה לא נכונה במשחקי המחשב אותן תופעות מתחילות בדרך כלל כאי נוחות קלה, אבל ללא שינוי בצורת הישיבה או בסידור עמדת המחשב יכולות להפוך לבעיה של ממש

טיפים לישיבה מול המחשב

המסך צריך להיות ממוקם ישר מולכם בגובה העיניים או טיפה נמוך ממנו-כך תשמרו על הצוואר שלכם.

אסור שמושב הכסא החלק התחתון שעליו אתם יושבים(ילחץ על אחורי הברך

בזמן הקלדה ועבודה עם העכבר שימו לב שנשמר קו ישר בין האמה וכף היד

המרחק המומלץ של המסך מכם הוא מרחק יד ישרה.

הידיים צריכות להיות לצידי הגוף מרפקים בגובה השולחן.

יש לשבת זקוף עם גב ישר על משענת הכסא

קו עליון של המסך
בגובה העיניים
כתפיים רפויות
ומרפקים קרובים לגוף
ידים מקבילות לקרקע
ונתמכות במשענות
ירכיים מונחות על
המושב לכל אורכו
משענת הכסא
תומכת בגב התחתון
זוית בין הירך לשוק
90 - 100 מעלות
זוית של כ- 105
בין המושב לבין
משענת הכסא
כל כף הרגל מונחת
על הרצפה
או על הדום רגליים