



תנאי בטיחות בשימוש באינטרנט למשפחות ולילדים

הורים יקרים,

אין ספק כי ילדינו גדלים היום במציאות שונה לחלוטין מזו שאנו גדלנו בה, כאשר לא היה מחשב והורינו דאגו רק שלא נפצע בחוץ. הילדים של היום, מאתגרים כל הזמן את הידע והאמונות שלנו בנוגע לטכנולוגיה ולאינטרנט ואת השילוב שלהם בחייהם.

רשת האינטרנט טומנת בחובה אוצר בלום ואינסופי של הנאה, תקשורת, שיתוף וידע, אך לצד אלה ישנן גם לא מעט סכנות. במדריך זה נסקור סכנות פוטנציאליות ברשת האינטרנט ונלמד על דרכים יעילות להתגבר עליהן ולסייע לכם ולילדכם לגלוש בהנאה ובביטחון.

אילו סכנות עלולות להיגרם משימוש באינטרנט?

הסיכון באינטרנט מחולק לשלושה סוגים עיקריים:

פשעי אינטרנט: וירוס או תוכנות זדוניות אחרות המתגנבות ללא ידיעתכם למחשב; הונאות מקוונות, כגון חטיפת זהות ופריצה לחשבונות דוא"ל ולרשתות חברתיות לצורך גניבת פרטי מידע אמיתיים ("שם, כתובות, מספר חשבון בנק, מספר כרטיס אשראי וכו'); תקיפות פיזיות או מקוונות על רקע מיני או שאינו מיני.

בעיות בין-אישיות: בריונות ברשת (שימוש של ילדים בהודעות דוא"ל, מסרים מידיים, תמונות, הודעות טקסט וכו' כדי להביך או להפחיד ילדים אחרים); חשיפה חד פעמית או קבועה לתכנים לא הולמים כגון אלימות, הסתה או מיין; התמכרות לפעילויות שונות באינטרנט (משחקים, הימורים וכו').

פגיעה במוניטין או בפרטיות: התחזות לאחר; פרסומים מוטעים או זדוניים על אדם או ילד ברשת; מעקבים ברשת ובחיים ה"אמיתיים"; גניבה והפרת זכויות יוצרים.



המלצות לשימוש בטוח באינטרנט להורים ולילדים

ההמלצות הבאות מובאות על פי חתך גילאי הילדים. מומלץ ליישם את ההמלצות הללו בצורה מצטברת, ככל שהילד מתבגר (ההמלצות לילד בן 5-7 נוגעות גם לילדים בני 8-12, אך לא תמיד ההיפך הוא הנכון).

ילדים בגילאי 5-7

שוחחו עם ילדיכם הקטנים ולמדו אותם על חשיבות ההגנה על מידע פרטי (שם, מספר טלפון וכו'). בצעו את ה"שיחה" באופן תמידי ולא רק באופן חד פעמי. הסבר ומהות ה"שיחה" מובאים בהמשך להמלצות. לדוגמא: הסבירו לא להשאיר פרטים אישיים בפרסומות מפתות, במיוחד מספרים ניידים אישיים, שכן אתם עלולים לשלם על זה מחיר כבד בעתיד.

הסבירו לילדיכם כי אין לשתף סיסמאות עם אחרים, אין למסור סיסמאות בדוא"ל לאף אחד, גם אם קבלתם מייל מחברה כי שם המשתמש שלכם נפרץ. זכרו כי הנהלת האתר לעולם לא תבקש מכם לשלוח סיסמאות אישיות במייל, ולכן הקפידו למחוק מיילים מסוג זה. כמו כן מומלץ לא למסור סיסמאות לחברים.

התקינו והקפידו לעדכן תוכנה לאבטחת אינטרנט: בין אם תוכנה נגד וירוסים או תוכנת הגנה מקיפה יותר, זכרו כי אבטחת נתונים הינה חשובה עד מאד. פנו לספק האינטרנט שלכם לרכישת תוכנת אנטי וירוס.

השתמשו בתוכנת בקרת הורים או שירות להגבלת גישה לאתרים מאושרים בלבד. תוכנת בקרת הורים מאפשרת להורים לבחור היכן ומתי ניתן לגלוש באינטרנט. קיימים יישומים רבים לבקרת הורים, ורמת הבקרה שונה בהתאם ליישום או לתוכנה, אך זו בדרך כלל כוללת רמות שונות של גלישה שניתן להתאים בהתאם לגיל הילד ולרצון ההורים.

ודאו כי הרשת האלחוטית שלכם מוגנת בסיסמה (במידה ולא, פנו אל המחלקה הטכנית של ספקית האינטרנט שלכם ובקשו לעדכן לכם סיסמה). רשת אלחוטית פתוחה תהפוך את מאמצי הפיקוח שלכם לקשים הרבה יותר. כמו כן, אם לאחד השכנים שלכם ישנה רשת אלחוטית "פתוחה" שניתן להתחבר אליה ללא סיסמה, כדאי להסביר לו את הסכנות הכרוכות בכך ולהציע לו לאבטח את הרשת בסיסמה. ודאו כי הרשת האלחוטית אינה מוגנת בסיסמת ברירת המחדל (משום שכך ניתן להתחבר אליה בקלות), אלא בסיסמה. דעו כי התחברות רבה של מחשבים לרשת אלחוטית שלכם עלולה לגרום לאיטיות בגלישה.

בדקו את ההיסטוריה של הדפדפן או תוכנת בקרת ההורים (בכל המחשבים בהם משתמשים הילדים כדאי לראות היכן הם גולשים ולפקח על הודעות דוא"ל ומסרים מיידיים, ולראות עם מי הם מתקשרים. שימו לב: אם הילד משתמש בטלפון נייד חכם (סמארטפון), הוא יכול לגלוש באינטרנט ולפעול ברשתות חברתיות גם ממכשיר זה, ומומלץ לשקול לחסום את הגלישה או להתקין בו אמצעי בקרה.

קבעו הגדרות אבטחה גבוהה לדפדפנים, חברויות, מנועי חיפוש ואתרי רשתות חברתיות. לדוגמה: Explorer Internet מציע הגדרות אבטחה ופרטיות תחת קטגורית "כלים" ואז "אפשרויות אינטרנט"; מנועי חיפוש פופולריים כגון גוגל מציעים גם תוכנות בטיחות כגון מסנן חיפוש בטוח (SafeSearch), המסיר תוצאות בעלות אופי מינימפורש.

הגדירו לילדיכם כללים ברורים לגלישה ברשת, שימוש ברשתות חברתיות, הורדות לא חוקיות ו"בריונות ברשת".

קיימו דיון עם ילדיכם על הסכנות הכרוכות בהעלאה ובשיתוף של מידע פרטי, תמונות וצילומי וידאו ברשת. ודאו כי ילדיכם מבינים כי אין להפוך את דף הרשת החברתית והפרטים האישיים שלהם לגלויים.

עודדו תקשורת פתוחה עם הילדים. עודדו אותם לספר - גם אם לא לכם, אז למורה, להורה, או למבוגר מהימן אחר - אם הם מרגישים לא נוח עם משהו שראו במחשב. ילדיכם צריכים לדעת שאסור ללחוץ על קישורים מאנשים לא מוכרים בתוך הודעת דוא"ל, מסרים מיידיים או רשתות חברתיות.



שימו לב לסממנים של התנהגות כפייתית או התמכרות למחשב, למשחקי און-ליין או לאינטרנט, כגון חוסר רצון או יכולת להפסיק, הזנחה של קשרי משפחה או חברים, שקרים לבני משפחה בנוגע לפעילות במחשב, בעיות בבית הספר או שינוי בדפוסי שינה.

ילדים בגילאי 13-17

חזקו את כללי ההתנהגות באינטרנט (שפה, פרטיות מידע, אתיקה, הורדות בלתי חוקיות, הגבלת שעות השימוש והימנעות מאתרים למבוגרים בלבד) היו מודעים לחיי החברה של בני הנוער ברשת (רשתות חברתיות, תצלומים, וידאו, מידע פרטי, פעילויות ספורט) באתרים שלהם, באתר של חברים, או בדפי האינטרנט של בית הספר.

בדקו את האתרים בהם מבקרים הילדים. אל תפחדו לדון יחד עם הילדים ואף להגביל את גישתם לאתרים שמדאיגים או פוגעים בכם. זכרו כי בני הנוער משתמשים באינטרנט בבית, בבית הספר, בבתי חברים, בספרייה, באמצעות הטלפון הנייד, רשתות אלחוטיות וגם באמצעות קונסולות משחק. דברו איתם על פעילותם בכל אלו.

הנחו אותם לא להוריד קבצים (מוסיקה, משחקים, שומרי מסך, רינגטונים) או לבצע עסקאות פיננסיות ללא רשות.

למדו את בני הנוער לבצע יציאה מסודרת מכל חשבון אליו הם נכנסו במחשב ציבורי או משותף לכמה אנשים.

השתדלו לשמור על מחשבים וטלפונים סלולריים של הילדים באזור משותף בבית ולא בחדר השינה.

אם אתם כמו רוב ההורים, אתם לא מומחים לאינטרנט או אפילו מיומנים כמו הילדים שלכם, זה בסדר, אין צורך להיות מומחים כדי שתוכלו לעזור לילדים ליהנות מהאינטרנט בבטחה. מה שצריך לעשות זה לדבר עם הילדים על מה שהם עושים באינטרנט ולקבוע יחדיו את הכללים לגלישה בטוחה.

לגרום לילדים שלכם לספר בכנות על החוויות שלהם באינטרנט, זה דבר קשה, אבל הכרחי. ככל שהילדים מתבגרים, הצורך שלהם בפרטיות גדל, אך גם הסיכונים שהם לוקחים באינטרנט עשויים לגדול. נטילת סיכונים היא חלק מתהליך ההתבגרות הטבעי. כהורים, תפקידנו הוא לסייע לילדים להגדיר גבולות, כדי שהסיכונים שהם נוטלים לא יפגעו במוניטין שלהם או בעתידם.

ה"שיחה" צריכה לכלול חמש שאלות עיקריות. חשוב להקפיד לתת לילד את המרחב (הן פיזית והן מבחינת הזמן) כדי לספק את התשובות לשאלות הללו. חשוב שהילד ידע שהוא מוגן מפני עונשים כדי שיענה תשובות אמיתיות.

שאלות ה"שיחה":

1. מה החברים שלך עושים באינטרנט?

שאלה זו מפנה את תשומת הלב מן הילד שלך כלפי פעילויות מקוונות כלליות בסביבה שלו. זוהי דרך טובה להתחיל את השיחה ולשמור על נייטרליות. מיד תתחילו לשמוע על פעילויות כגון משחקים, צ'אטים, רשתות חברתיות ובתקווה גם שיעורים ופעילויות מחקר.

2. מהם אתרי האינטרנט המגניבים או החדשים?

בקשו מהילד לספר למה האתרים האלה מגניבים. תוכלו גם לשאול על אתרים שאינם פופולאריים יותר (אתם בטח מכירים כמה כאלו, תקוו שהילד מכיר...) ומדוע הם לא פופולאריים.

3. במה אתה משתמש הכי הרבה? רוצה להראות לי את האתרים המועדפים עליך?

שאלו את הילד כיצד הוא מגדיר את הגדרות האבטחה והפרטיות (הסתכלו על החלק העליון והתחתון של אותם אתרים). שאלו את הילד כיצד הוא משתמש באתר ולמה הוא מעדיף אתר מסוים על פני אתר אחר.

4. האם שמעת על "בריונות ברשת" והאם אי פעם חווית זאת?

הילד שלכם (ואולי גם אתם) לא יכול לדעת מה משמעות "בריונות ברשת" רק לפי השם, אבל הוא בוודאי יודע כיצד זה נראה ומרגיש. דברו איתו על סיפורים ששמעתם בנוגע להטרדות בדוא"ל או ברשתות חברתיות, תמונות מביכות או מידע אישי שנחשף או נשלח לילדים אחרים. שאלו את הילד על זיוף פרופילים ברשת החברתית. ברו עם הילד האם כבר שמע או ראה סוג כזה של התנהגות. ודאו כי הילד מבין ויודע ש"בריונות ברשת" נפוצה מאוד ואם הוא לא ראה זאת, זה רק עניין של זמן עד שייפגש בסוג כזה של התנהגות. ודאו שהילד יודע איך להגיב כאשר היא מתרחשת, לא צריך להגיב על כל דוא"ל או צ'אט המכיל "בריונות"; צריך לנסות לשמור או להדפיס את התכתובת, צריך לחסום את ה"בריון".

5. יש באינטרנט משהו שאי פעם גרם לך להרגיש מוזר, עצוב, פוחד או לא נוח?

זוהי הזדמנות לדון שוב ב"בריונות ברשת", בתגליות גלישה מקריות או חוזרות כמו אלימות, פורנו או אתרים גזעניים או אפילו משהו מוזר שקרה לחבר בשכונה. הרעיון הוא לוודא שהילד שלכם ידע שהוא יכול לבוא אליכם והוא לא יענש כאשר משהו יוצא דופן או רע קורה באינטרנט. חוויה של משהו רע היא כמעט בלתי נמנעת כאשר הילד שלכם פעיל באינטרנט, ולכן חשוב שתוודאו שהילד יודע שהוא יכול לפנות אליכם לעזרה ושאתם לא תגזימו בתגובה.

זה הכל. זו בסך הכל שיחה. לא קשה, לא טכנית וברת ביצוע לחלוטין.