

מדריך כללי זהב להתנהלות בטוחה ברשת

מה חשוב לדעת?
ממה כדאי להיזהר?
כיצד מומלץ לנהוג?



שלום רב,

לכבוד חודש המודעות הלאומי לסייבר, החל בחודש אוקטובר, אנו שמחים לשתף עמכם מדריך שימושי הכולל עצות פשוטות ליישום עבור המשתמשים (כולנו למעשה) ברשת האינטרנט. במיוחד בימים אלה, כאשר מכורח המציאות גובר השימוש בשירותים מקוונים ובתקשורת מרחוק, אנו ממליצים לעיין במדריך ולהקפיד ליישם את ההמלצות המפורטות בו על מנת להמשיך וליהנות בבטחה מהיצע השימושים של הרשת.

אתם יותר ממוזמנים לשתף ולהפיץ את הקובץ ולעזור בהפצת המודעות לסיכוני הסייבר ברשת והאמצעים להגנה מפניהם.

בברכה,

מרכז הגנת הסייבר BDO

* המדריך כתוב בלשון זכר אך פונה לשני המינים

צור סיסמה אשר אינה ניתנת
לפיצוח בקלות

**סיסמה
חזקה**



היכנס רק לאתרים
מוכרים ואמינים

**גלישה
בטוחה**



התייחס בחשדנות וזהירות למסרונים
ודואר אלקטרוני ממקור לא ידוע, במיוחד
הודעות עם קישור לחיפה לאינטרנט

**הודעות
חשודות**



נעל את המכשיר בתום השימוש;
וודא שקיים אנטי-וירוס במחשב ובטלפון;
דאג לגיבוי המידע החשוב לך

**הגנה
וגיבויים**



היה זהיר בשיתוף מידע עם
גורמים אשר אינם מוכרים לך

פרטיות



שמור על פרטייך הפיננסיים
בדיסקרטיות יתרה;
רכוש ובצע תשלומים אך ורק
באתרים מוכרים וידועים

**תשלום
ומידע
פיננסי
ברשת**



סיסמה חזקה



בדיוק כפי שאנו שומרים על תכולת כספת באמצעות קוד, כך חשוב להגן על המידע הפרטי והאישי שלנו באתרים השונים באמצעות סיסמה חזקה שתבטיח לנו גישה בלעדית אליהם.

כל עוד סיסמה זו תהיה מורכבת מפרטים אשר ידועים עלינו (לדוגמא: שם פרטי, משפחה, מספר טלפון, תאריך לידה וכדומה), הדבר יקל על ניחושה וכפועל יוצא את הגישה לחשבונות.

מה כדאי לעשות?

- יש ליצור סיסמה קשה לניחוש עבור המחשב, הרשת האלחוטית והאתרים השונים בהם אנו מנהלים חשבונות (בנק, מרפאה, פייסבוק, ZOOM ועוד).

ליצירת סיסמה חזקה וקשה לניחוש מומלץ לשלב אותיות גדולות וקטנות באנגלית, ספרות וסימנים.

סיסמה חזקה לדוגמא: **Bvz85\$**

- מומלץ מאוד:** באתרים רגישים מאוד כמו בנק או קופת חולים, יש להיעזר בהגנת קוד נוסף אשר נשלח כהודעה לטלפון בכל פעם שאתם מתחברים; כך במידה והפורץ גילה את סיסמתכם, לא תהיה לו אפשרות להיכנס לאתר ללא הקוד מהטלפון.

גלישה בטוחה



בזמן גלישה ברשת אנו נתקלים לא אחת באתרים המבקשים מאתנו "להוריד" קבצים למחשב או מכנים ללחיצה על קישורים. במידה ומדובר באתר שאינו מאובטח לשימוש, קיימת סכנה ממשית לפריצה והשתלטות על ידי גורמים בלתי רצויים בעת הלחיצה על הקישורים.

מה כדאי לעשות?

- לגלוש רק לאתרים מוכרים ולשמור אותם בסרגל המועדפים.
- בעת הגלישה באתרים חדשים, יש לוודא בשורת הכתובת שהאתר מאובטח (סימון של מנעול סגור).
- יש לגלוש לאתרים רגישים (קופת חולים, ביטוח, בנק) מהבית ורק מהטלפון והמחשב האישיים.

הודעות חשודות



שיטה נפוצה בשנים האחרונות בה נוקטים גורמים זדוניים, היא לשלוח מסרון או דואר אלקטרוני המכיל בקשה למסירת מידע אישי ולחיצה על קישור.

זכרו! בנקים, חברות ביטוח, קופות החולים וגופים רגישים אחרים לעולם לא יבקשו את הסיסמה שלכם. אם מישהו מבקש זאת מכם, זו היא נורה אדומה ועליכם לחשווד ולהימנע ממסירת הפרטים.

מה כדאי לעשות?

- אין למסור מידע רגיש בקבלת שיחה מגורם בלתי מזוהה.
- אין ללחוץ על קישורים שהגיעו בדואר אלקטרוני או במסרון מגורם לא מוכר. גם אם נדמה שמכירים ויש ספק קטן, עדיף להימנע ולהתייעץ עם גורם שאתם סומכים עליו.

גיבויים והגנה



לצד העובדה שאנו צוברים מידע רב במחשב ובטלפונים הניידים שברשותנו, במקרים רבים עלול המידע להימחק או להגיע ל"ידיים הלא נכונות". גיבוי המידע והתקנת אנטי-וירוס יכולים לסייע משמעותית בהגנה על המידע היקר שלנו.

מה כדאי לעשות?

- להשתמש בקוד נעילה לטלפון הנייד ולנעול / לכבות את המחשב בסיום השימוש.
- לוודא שהמערכת והאפליקציות שלכם מתעדכנות אוטומטית במחשב ובטלפון הנייד; העדכונים מכילים הגנות חדשות ועוזרים למנוע פריצה.
- לוודא שקיים אנטי-וירוס על-גבי הטלפון הנייד והמחשב.
- התקנת גיבוי אוטומטי עבור כל המידע בטלפון הנייד.



השימוש באמצעים טכנולוגיים מלווה אותנו לצרכים רבים בחיי היומיום שלנו, כגון פעולות אל מול הבנק, קשר עם המרפאה, ביצוע פעולות וקבלת מידע מהביטוח הלאומי, קניות, שיחות עם בני המשפחה, הכרת חברים חדשים וכן אתרי פנאי ומשחקים. פעולות אלו מצריכות מאתנו לרוב מסירת מידע אישי.

שימו לב: כמעט כל מידע שאנו משתפים ברשת, עשוי להיות ציבורי ולהתגלות לעיני כל. חשוב לקרוא את מדיניות הפרטיות באתרים ולזכור כי ככל שנשתף פחות מידע אישי, יופחת הסיכון לשימוש לא ראוי בו על ידי גורם בלתי רצוי.

מה כדאי לעשות?

- עצור והפעל שיקול דעת בגין טיב האתר ומטרתו לפני שיתוף בפרטים אישיים או פיננסיים אודותיך או אודות הקרובים לך.
- מומלץ למסור פרטים אך ורק באתרים מוכרים.

תשלום ומידע פיננסי ברשת



קניות באמצעות אתרי אינטרנט שונים הפכו נפוצות בקרב כלל האוכלוסייה. היצע האתרים התרחב בכל תחומי הצרכנות; לפיכך, חשוב מאוד להיות זהירים ולנקוט במשנה זהירות בתהליך הרכישה ברשת אשר כולל כמובן הכנסת מספר כרטיס אשראי או אמצעי תשלום אחר שברשותנו.

מה כדאי לעשות?

- כדאי לוודא שהאתר מאובטח ע"י בדיקת סרגל הכתובת והופעת מנעול (במידה והאתר לא מאובטח, יופיע מנעול אדום ועליו X).

 | <https://>

- בעמוד הכנסת פרטי התשלום, חפשו אות סמל תו התקן הנועד להבטיח שהאתר מגן על פרטי כרטיס האשראי.



רשימה מרוכזת של ההמלצות

<p>יש ליצור סיסמה קשה לניחוש עבור המחשב, הרשת האלחוטית והאתרים השונים בהם אנו מנהלים חשבונות (לדוגמא: \$Bvz85).</p> <p>באתרים רגישים מאוד כמו בנק או קופת חולים, יש להיעזר בהגנת קוד נוסף אשר נשלח כהודעה לטלפון בכל פעם שאתם מתחברים.</p>	סיסמה חזקה
<p>לגלוש רק לאתרים מוכרים ולשמור אותם בסרגל המועדפים.</p> <p>בעת הגלישה באתרים חדשים, יש לוודא בשורת הכתובת שהאתר מאובטח.</p> <p>יש לגלוש לאתרים רגישים (קופת חולים, ביטוח, בנק) מהבית ואך ורק מהטלפון והמחשב האישיים.</p>	גלישה בטוחה
<p>אין למסור מידע רגיש בקבלת שיחה מגורם בלתי מזהה.</p> <p>אין ללחוץ על קישורים שהגיעו בדואר אלקטרוני או במסרון מגורם לא מוכר.</p>	הודעות חשודות
<p>להשתמש בקוד נעילה לטלפון הנייד ולנעול או לכבות את המחשב בסיום השימוש.</p> <p>לוודא שהמערכת והאפליקציות שלכם מתעדכנות אוטומטית במחשב ובטלפון הנייד העדכונים מכילים הגנות חדשות ועוזרים למנוע פריצה.</p> <p>לוודא שקיים אנטי-וירוס על-גבי הטלפון הנייד והמחשב.</p> <p>התקנת גיבוי אוטומטי עבור כל המידע בטלפון הנייד.</p>	גיבויים והגנה
<p>עצור והפעל שיקול דעת בגין טיב האתר ומטרתו לפני שיתוף בפרטים אישיים או פיננסיים אודותיך או אודות הקרובים לך.</p> <p>מומלץ למסור פרטים אך ורק באתרים מוכרים.</p>	פרטיות
<p>כדאי לוודא שהאתר מאובטח ע"י בדיקת סרגל הכתובת והופעת מנעול (במידה והאתר לא מאובטח, יופיע מנעול אדום ועליו X).</p> <p>בעמוד הכנסת פרטי התשלום, חפשו את סמל תו התקן הנועד להבטיח שהאתר מגן על פרטי כרטיס האשראי.</p>	תשלום ומידע פיננסי ברשת

אודות BDO

BDO ישראל הינה פירמת ראיית חשבון ויעוץ עסקי דינמית ובעלת אוריינטציה עסקית, הנמנית על חמש הפירמות הגדולות בישראל. הפירמה נוסדה בשנת 1983 כחלק מהרשת הבינלאומית BDO ומפעילה עשרה סניפים ברחבי הארץ, וכמו כן, דסקים ישראלים בסין, הודו, וייטנאם, ארה"ב ויוראסיה. הפירמה מעסיקה כיום בישראל מעל 1,600 עובדים ומספקת שירותים למגזר הפרטי, הציבורי והממשלתי ומטפלת בלמעלה מ-300 חברות ציבוריות וקרנות שונות, הנסחרות בבורסות בארץ ובעולם.

אודות מרכז הגנת הסייבר של BDO

מרכז הגנת הסייבר של BDO (SECOZ) (לשעבר), מוביל בתחום הגנת הסייבר ואבטחת המידע בארץ ובחו"ל מאז שנת 2002. המרכז צבר בשנות פעילותו הרבות, ניסיון עשיר אל מול השוק הבינלאומי והמקומי, במגוון רחב של מגזרים, ביניהם פיננסים, תעשייה, ממשלה, הייטק, תשתיות, סטרטאפים ובריאות.

השילוב בין מומחיות בתחומי הסייבר ואבטחת המידע לבין מומחיות בתחומי האסטרטגיה וניהול הסיכונים, מאפשרים לצוות מרכז הסייבר לספק לכל לקוח מענה הוליסטי בגישה ייחודית. צוות המומחים שלנו מבין לעומק את התהליכים והדרישות העסקיות של כל לקוח ויודע לשזור אותם בד בבד עם הדרישות והצרכים הטכנולוגיים. באופן זה, בידינו להתאים את הפתרונות האידאליים עבור כל לקוח, סביבה, מטרה וצורך תוך שמירה על האינטרסים והפעילות העסקית.

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO Israel to discuss these matters in the context of your particular circumstances.

This publication is confidential, protected by copyright and may be privileged. It is for the exclusive use of the intended recipient(s).

BDO Israel, its partners, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO Israel, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independence Member Firms.

BDO is the brand name for the BDO network and for each of BDO Member Firms.

For further information about how BDO can assist you and your organization, please visit www.bdo.co.il