

גולשים ברשת, נזהרים ונהנים

אגרת מידע (לא רק) לאזרחים ותיקים

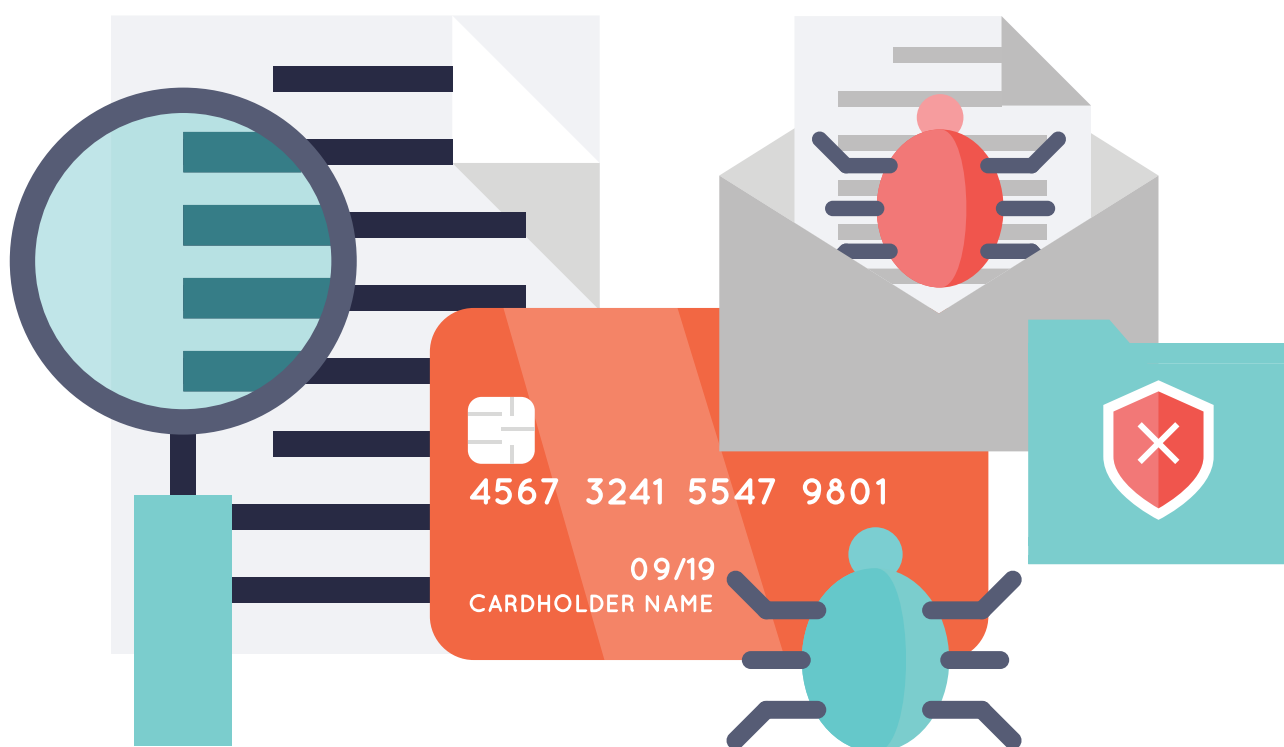


האמצעים הדיגיטליים - האינטרנט, הטלפון החכם והמחשב - מאפשרים הזדמנויות רבות ליצירת קשר, ללמידה, להנאה וליצירה. לצד ההנאה מהעושר הקיים בהזדמנויות האלה, חשוב ללמוד איך גולשים בבטחה מבלי להיפגע מהסכנות הקיימות באמצעים הדיגיטליים. באיגרת זו נסקור דרכים לגלישה בטוחה ונסביר כיצד אפשר להימנע מסכנות נפוצות.



זהירות, וירוס!

וירוס בעולם הדיגיטלי דומה לווירוס במציאות. הוא עלול להרוס את המחשב או את הטלפון החכם שלנו, ולעיתים גם לאפשר לגורמים פליליים לאסוף עלינו מידע ולהשתמש בפרטים האישיים שלנו. נדבקים בוירוס בעיקר באמצעות לחיצה על קישורים והורדת תוכנות.



איך נזהרים?

1. קיבלתם קישור (לינק) בהודעת SMS, בוואטסאפ, בדוא"ל או בצ'ט

הקדישו תשומת לב לזיהוי השולח של המייל או ההודעה. גם אם נראה שההודעה ממוענת אליכם באופן אישי, שאלו את עצמכם: האם אתם מכירים את מי ששלח?



לפני שאתם לוחצים על הקישור, או מורידים קובץ שמצורף להודעה, שלחו הודעה חזרה לשולח ושאלו אותו אם אכן הוא העביר את הקישור (לינק) או הקובץ ואם מדובר בתוכן בטוח.



אל תפתחו את ההודעה, אל תמסרו פרטים אישיים ואל תפיצו את ההודעה הלאה. מומלץ למחוק את ההודעה הזאת.

2. התקנת תוכנות ואפליקציות בטלפון החכם או במחשב

נקפיד להתקין תוכנות ואפליקציות מאתרים רשמיים בלבד. כך למשל כדי להתקין תוכנות במחשב, יש לעשות זאת מהאתר של Microsoft או מחנות האפליקציות של Google, שנחשבים לאתרים אמינים, וכדי להתקין אפליקציות לטלפון החכם, יש להשתמש לשם כך רק בחנות האפליקציות (חנות Play באנדرويد ו-App store באייפון).

אם יש ספק, אין ספק!

יש להימנע מלהוריד תוכנה שאנחנו לא בטוחים לגביה.

תוכנה שכן כדאי להוריד היא תוכנות אנטי-וירוס שתסייע לנו בהגנה על המכשיר. כדאי להתקין על המחשב והטלפון החכם תוכנת אנטי וירוס, ולהגדיר בהם סריקה אוטומטית לאיתור וירוסים פעם ביום (אפשר להיעזר באיש מקצוע לשם כך).



סיסמאות

אחד הכלים היעילים ביותר להגן על עצמנו הוא בחירת סיסמאות חזקות לכל היישומים (אפליקציות) והאתרים שאנו גולשים בהם. **חשוב שהסיסמה לא תכיל פרטים אישיים** - כגון שם פרטי, שם משפחה, תאריך לידה, מספר תעודת זהות, מספר טלפון או מספר חשבון בנק.

- חשוב להגדיר סיסמה שונה לכל יישום (דוא"ל / בנק / פייסבוק / קניות וכדומה).
- אין לשמור סיסמאות בטלפון הנייד, מחשב שהמכשיר ייגנב.
- מומלץ לרשום את הסיסמאות בדף מסודר ולהניחו במקום בטוח ורחוק מהמחשב.
- מומלץ להחליף סיסמאות כל שישה חודשים.



סיסמאות - המשך

קיבלתם הודעה או דוא"ל מחברה עסקית, קופת חולים, משרד ממשלתי, בנק, פייסבוק וכיוצא באלה, ובה מבקשים ממכם לעדכן פרטי תשלום, סיסמה או פרטים אישיים כמו כתובת ותעודת זהות?

לעולם אין למסור סיסמאות ופרטים אישיים לגורם שיזם אליכם את הפנייה, במיוחד אם ההודעה כוללת טון של דחיפות - למשל שחשבוך ייחסם תוך 12 שעות.

זכרו, הפרטים של כל לקוח או משתמש הם קבועים עד אשר הלקוח מבקש מיוזמתו לשנות אותם. אפשר לוודא שלא מדובר בהודעה אמיתית על-ידי שיחה טלפונית לגורם ששלח אותה לכאורה.



קניות באינטרנט

הקניות באינטרנט יכולות להקל על ההתנהלות שלנו, לחסוך לנו זמן ולעיתים גם עלויות. עם זאת, יש לשים לב לכמה נושאים לפני שקונים.

- **העדיפו לרכוש מחנויות שאתם מכירים ושנכנסתם אליהן מיוזמתכם**, למשל דרך חיפוש בגוגל ולא בעקבות לחיצה על פרסומת.

- אם בכל זאת הגעתם לחנות שאתם לא מכירים, חפשו עליה מידע באינטרנט ובעיקר ביקורות של לקוחות קודמים. בדקו שיש לחנות כתובת פיזית תקינה ואפשרות ליצור קשר באמצעות מספר טלפון.

- **השוו מחירים** - אם המחירים באתר נמוכים מאוד, אנו עלולים להתפתות אבל כדאי לחשוד. לכן כדאי להשוות מחירים לפני כל קנייה. אתרים מומלצים להשוואה:

www.zap.co.il, www.kamaze.co.il, www.wisebuy.co.il




קניות באינטרנט - המשך

- חפשו את **המנעול הירוק או שחור** המופיע בשורה של כתובת האתר כדי לוודא שהאתר מאובטח וששומרים בו על פרטי כרטיס האשראי שלכם. וודאו שכתובת האתר מתחילה באותיות **https**. שימו לב להבדלים בכתובות האתרים בין אתר מאובטח ללא מאובטח:

לא מאובטח

www.shopping.co.il

מאובטח

 https://shopping.co.il

הודעת פרסומת / מבצע

אם לא זכור לכם שנרשמתם למועדון או לרשימת התפוצה של החנות, עדיף להימנע מללחוץ על קישור שנשלח אליכם. מתעניינים במבצע? אתם יכולים להיכנס לחנות דרך הדפדפן (גוגל) ולבדוק האם המבצע הזה מופיע באתר של החנות.

הונאות בטלפון ובדוא"ל

הונאות בטלפון ובדוא"ל מיועדות בדרך כלל לקבלת כסף באופן ישיר מכם או באמצעות פרטים אישיים שתמסרו.

כיצד להימנע מהונאות כאלה:

• **מישהו התקשר אליכם, מציע לכם הצעה אטרקטיבית ולוחץ עליכם לקבל החלטה?**

אנחנו ממליצים בחום להימנע מרכישה טלפונית, אפילו כשמדובר בגוף מוכר כמו חברת ביטוח או סלולר.

אם קשה לכם להתמודד עם לחץ מהצד שפנה אליכם, אמרו שעליכם להתייעץ עם הילדים או עם בן/בת הזוג ונתקו את השיחה.

• **מישהו התקשר ומבקש לוודא איתכם פרטים אישיים?**

אמרו לו שאתם תצרו קשר חזרה עם החברה כדי למסור את הפרטים ונתקו את השיחה.



הונאות בטלפון ובדוא"ל - המשך

• מישהו מתקשר, לכאורה בשם בן משפחה או מכר שלכם, ומבקש עזרה כספית או אחרת?

בקשו שיחזור אליכם עוד חצי שעה ונתקו את השיחה. התקשרו לאותו בן משפחה / מכר או לקרוביו ודרשו בשלומם.

• מישהו שלח לכם דוא"ל, ובו בקשה דחופה לסיוע כלכלי מסיבה כלשהי (למשל עבור אדם זר או בן משפחה שחולה, נתקע במדינה זרה וצריך כסף לחזור לארץ)?

אל תשיבו לדוא"ל. אם מדובר באדם מוכר, צרו קשר טלפוני עימו ודרשו בשלום האדם שהוזכר בפנייה. במרבית הפעמים אותו אדם לא מודע לכך שבקשות כאלה מופצות בשמו.



אתרים מתחזים

כאשר אנחנו גולשים באינטרנט, חשוב לשים לב שלא הגענו לאתר מתחזה, ש"מתחפש" לאתר אחר. לעיתים יכולה להופיע כתובת דומה מאוד לאתר האמיתי ושיש בה שינוי של תו אחד. כך למשל אתר החדשות Ynet.co.il יכול להופיע כ- Ymet.co.il ולהכיל קישורים זדוניים. לחלופין, אתר ממשלתי, כמו הר הכסף למשל, יופיע בסיומת co.il במקום סיומת gov.il, שהיא הסיומת הממשלתית הרשמית, וכך יגבה במרמה תשלום על שירות ממשלתי שמוצע בחינם.

מה עושים?

נקרא בתשומת לב את שורת כתובת האתר בדפדפן, ונוודא שהיא נכונה. שימו לב שההתחלה או הסיומת בכתובת האתרים של משרדי הממשלה היא gov.il, ואילו הסיומת בכתובת האתרים של הרשויות המקומיות היא muni.il.

www.gov.il/he/subjects/certificates_and_passports

ידיעות כזב (פייק ניוז)

אחת התופעות שמאפיינת את העת האחרונה היא ריבוי ידיעות המפיצות מידע לא מבוסס ואף שקרי. ידיעות כאלו עלולות לגרום לפחד מיותר או לשאננות מסוכנת.

מה עושים?

• הטילו ספק בידיעה שנשמעת לכם קיצונית מידי או מפתיעה לגורם שהיא מיוחסת אליו.

• אפשר להצליב את המידע מול מידע המפורסם באתרים רשמיים, כגון משרד הבריאות ומשטרת ישראל, ובאתרי חדשות אמינים או להתייעץ עם קרוב משפחה או חבר. אפשרות נוספת היא לבדוק את הידיעה באתר "לא רלוונטי"

www.irrelevant.org.il

לסיכום

חשוב לזכור שכולנו, צעירים כמבוגרים, יכולים ליפול קורבן להונאות ברשת, ואין במה להתבייש! נוכל להנות מגלישה מהנה, מועילה ובטוחה, אם נלמד להיזהר מהסכנות הנפוצות, נזהר בלחיצה על קישורים ונמנע לחלוטין ממסירת פרטים אישיים.

אם נתקלתם בהונאה, אנא דווחו לנטיקה מבית ארגון האינטרנט הישראלי באחד מן האמצעים הבאים:

בשיחה או בהודעת וואטסאפ למספר הטלפון 054-8858911

בדוא"ל safe@isoc.org.il

בטופס דיווח <https://www.isoc.org.il/netica/report>

כך תוכלו לסייע לאחרים ולמנוע את ההונאה הבאה.

איגרת זו נערכה על-ידי דידי בן שלום, ד"ר מיכל הלפרין בן צבי וליאת סקרון בשיתוף פעולה בין ג'וינט ישראל-אשל ומטה המיזם הלאומי "ישראל דיגיטלית" במשרד הדיגיטל הלאומי לבין איגוד האינטרנט הישראלי (ע"ר) כחלק מהמיזם הלאומי לקידום אוריינות דיגיטלית בקרב אזרחים ותיקים (2020). למידע נוסף, בקרו באתר הידע של המיזם:

<http://digitalcampus.co.il/>

איגוד
האינטרנט
הישראלי
ISOC-IL



ג'וינט ישראל אשל
יחד בעשייה חברתית למען הזקנים

