



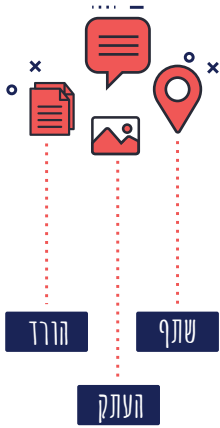
איסוף מידע ומודיעין - לא להיות חשופים ברשת!

עמוד 1 מתוך 2



כלים להתנהלות בטוחה ברשת

פרסום ושיתוף מידע אישי



מודעות זה שם המשחק! חשוב להתרגל לעצור ולחשוב לפני כל פרסום פוסט, העלאת תמונה או שיתוף מידע.

מידע אישי? שיישאר פרטי! לא לפרסם בפומבי מידע אישי כמו מספרי טלפון, גיל, כתובת מגורים, אימייל וכדומה, גם אם הפרופיל הוא פרטי.

עבור מה שבחרת לפרסם - חשוב להגביל את ההרשאות לצפייה בפרטים שלך.

למחוק זה לא צחוק! חשוב למחוק את כל המידע המיותר מהפרופילים שלך.

לא הכרת!? לא אישרת! לאשר ברשתות החברתיות חברות רק לאנשים אותם מכירים ולא להתפתות לאשר פרופילים חשודים.

באיזה פרופיל צריך לחשוד?

- פרופיל ללא תמונה או עם תמונת ברירת מחדל
- שימוש בתמונה של דוגמנים/דוגמניות או של פרופילים קיימים
- פרופיל שנוצר לאחרונה
- ביוגרפיה ריקה בפרופיל
- שכפול פוסטים - חזרה על אותם פוסטים או פוסטים דומים מאוד
- פרופיל עם מעט חברים (מתחת ל-50)

הרשאות גישה

לא לאשר אוטומטית!



לבחון אילו הרשאות גישה נדרשות בהורדת אפליקציות ובהרשמה לאתרים/שירותים מקוונים, ולאשר גישה אך ורק למידע שנחוץ למטרה שלהם.

חשוב לקרוא את מדיניות הפרטיות של האפליקציה כדי לקבל תמונה מלאה על מה שקורה למידע שלך ולהחליט לפיה.

כדאי לבצע בדיקת פרטיות והרשאות גישה באפליקציות ואתרים שמאפשרים זאת. הבדיקה מציגה את המצב הנוכחי שלך ומאפשרת לעדכן את ההרשאות על פי הצורך.

בעבודה עם אנשים, חשוב מאוד לתת הרשאות רק לאנשים הנדרשים ולצורך מילוי תפקידם בלבד! גם אם מספר אנשים צריכים הרשאה לאותה תיקייה, הגישה לקבצים או מסמכים בתיקייה לא בהכרח זהה לכולם.

עבור עסקים

מומלץ לרכוש תוכנה לניהול הרשאות גישה בארגון/בקבוצה.

אם העסק שלך מנהל עמודים ברשתות חברתיות או באתרים אחרים, יש לוודא שהגדרות הפרטיות חלות עליהם בצורה תקינה ושמידע עסקי רגיש לא חשוף לעיני כל.



איסוף מידע ומודיעין - לא להיות חשופים ברשת!

עמוד 2 מתוך 2



גלישה ברשתות אלחוטיות

בכל המקרים של התחברות לרשת אלחוטית חשוב להקפיד על התחברות מאובטחת באמצעות סיסמה חזקה.



תמיד עדיף להתחבר לרשת Wi-Fi פרטית.

כאשר אין אפשרות להתחבר לרשת Wi-Fi פרטית, אפשר להתחבר לאינטרנט באמצעות:



1. (אפשרות מועדפת) Hotspot אישי מהטלפון הנייד שלך או של אדם עליו סומכים.

2. רשת Wi-Fi ציבורית, ולהקפיד:

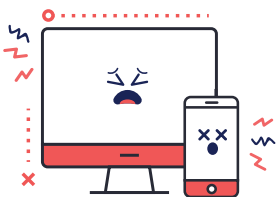
• לא להתחבר אוטומטית לרשתות Wi-Fi (אפשר להגדיר במכשיר)

• לא לבצע פעולות רגישות או להעביר מידע רגיש

• לגלוש רק באתרים מאובטחים (מסומנים במנעול סגור וכתובתם מתחילה ב-https)



3. נטסטיק



הכנת מכשיר אלקטרוני לטיפול

במקרה של מסירת מכשיר לטיפול או השתלטות על המכשיר מרחוק יש להכין את המכשיר כך שהמידע שלך לא יהיה חשוף במהלך הטיפול/ההשתלטות מרחוק.

לצורך כך יש להקפיד על הסעיפים הבאים:

• לגבות את המידע על גבי כונן חיצוני ובענן.

• למחוק את המידע שאינו נחוץ לך.

חשוב במיוחד למחוק קבצים שנמצאים בשולחן העבודה שלך (Desktop).

• למחוק מהדפדפן את קובצי העוגיות ואת היסטוריית הגלישה שלך.

• לנעול את הגישה למידע הרגיש שבמכשיר באמצעות סיסמה או אמצעי הזדהות אחר.

להתנתק מהחשבונות שלך (ג'מייל, פייסבוק וכדומה).

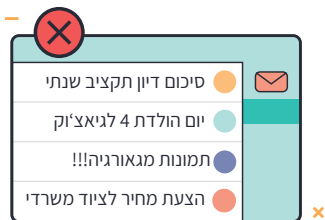
חשוב לזכור לגבות את המידע באופן אוטומטי ולעיתים קרובות גם למקרים בהם המכשיר מתקלקל ומושבט באופן שלא מאפשר לגבות את המידע שבו לפני המסירה לטיפול.

שימוש בחשבונות אימייל

"הפרד ומשול"

• להפריד בין חשבונות אימייל לצרכים שונים: חשבון אימייל פרטי וחשבון אימייל של מקום העבודה. להגדיר לכל אחד מהחשבונות סיסמה חזקה ושונה.

• להקפיד להשתמש בכל תיבת אימייל לצרכים שלה בלבד.



שליחת אימייל דורשת תשומת לב מירבית!

• לשים לב שהקלדת את כתובת האימייל הנכונה של הנמען.

• כששולחים מייל לתפוצה רחבה להקפיד להפיץ לכולם דרך "עותק מוסתר".

יש לך כתובת אימייל עסקית?

מומלץ לפתוח תיבת אימייל כללית נפרדת לניהול התכתובות מול לקוחות/ספקים, לפניית לחברה (כמו "צור קשר"), הפצת פרסומים וכדומה. מומלץ שיהיה גם מספר טלפון אחד/מרכזיה שיתן מענה לפנייה לאנשים בארגון.